

SUPREMO AMICUS

INDIA'S FIRST AI INTEGRATED LAW JOURNAL

Peer Reviewed, Refereed and Open access Journal

- Available in 331+ International Libraries
- Indexed at 32 Databases



ISSN NO. 2456-9704
Volume 10 Issue 3
www.supremoamicus.org



DISCLAIMER

The information presented in this article is intended for general informational and educational purposes only. While every effort has been made to ensure that the content is accurate, up-to-date, and reliable at the time of publication, the editorial board and publisher make no representations or warranties of any kind, express or implied, regarding the completeness, accuracy, reliability, suitability, or availability of the information contained herein.

The views and opinions expressed in this article are those of the author and are based on personal research, experience, and interpretation. They do not necessarily reflect the official policy, position, or opinions of any affiliated organization, institution, or entity.

This article is not intended to serve as professional advice of any kind. The editorial board and publisher shall not be held liable for any errors or omissions in the content, nor for any losses, injuries, or damages arising from the use of or reliance on this information.



ABOUT THE JOURNAL

Supremo Amicus is an online, peer-reviewed international journal devoted to the interdisciplinary fields of law and science. In an era marked by rapid technological progress and evolving legal frameworks, the journal seeks to bridge the gap between these two dynamic domains by offering comprehensive and critical insights into their various aspects. The journal places a strong emphasis on contemporary advancements, emerging trends, and the complex challenges faced by both the legal community.

The primary objective of the journal is to encourage and promote original, high-quality research. It is committed to publishing well-researched, analytically sound, and thought-provoking articles that adhere to rigorous academic standards. Each submission undergoes a thorough peer-review process to ensure authenticity, relevance, and scholarly integrity. In doing so, the journal maintains its commitment to excellence and credibility.

In addition to fostering research, the journal aims to make complex ideas accessible and engaging for a diverse readership. It strives to present content that is not only intellectually enriching but also clearly written and reader friendly.

Furthermore, the journal is committed to promoting interdisciplinary collaboration and global engagement. It welcomes diverse perspectives from contributors across different regions and backgrounds, thereby enriching the quality and scope of discussions presented within its pages.

With this vision we proudly present Supremo Amicus to our readers.

**-Editorial Team
Supremo Amicus**



“DIGITAL AUTONOMY AND INFORMATIONAL SELF-DETERMINATION UNDER ARTICLE 21: EMERGING CHALLENGES IN THE ERA OF ARTIFICIAL INTELLIGENCE”

By *Rachana Gupta*

Research Scholar (Law), Bundelkhand University, Jhansi (U.P.),

By *Dr. Rajendra Prasad*

Assistant professor at Bundelkhand College, Jhansi (U.P.)

Abstract

The blistering growth of artificial intelligence (AI) has been a fundamental change in the framework of informational power that raises urgent constitutional questions about the digital autonomy and privacy of individuals. Article 21 of the Indian Constitution, which was understood judicially to incorporate the right to life and personal liberty, has undergone a process where informational privacy has been found to be an inherent part of human dignity. The landmark decision in *Justice K.S. Puttaswamy v. Union of India* 2017 privacy became constitutionalized and a normative background was developed on informational self-determination recognition. Nevertheless, with the advent of algorithmic governance, predictive analytics, biometric surveillance and automated decision-making systems pose more challenges to this constitutional guarantee than ever before.

It states that the traditional principles of privacy (identified as the focus on consent and data control) are insufficient in solving the structural asymmetries inherent in AI systems.

Keywords: Digital Autonomy; Human Dignity; Informational Self-Determination; Article 21; Artificial Intelligence; Algorithmic Governance; Informational Privacy; Proportionality Doctrine.

1. INTRODUCTION

1.1 Background and Context

The successful spread of digital technologies and artificial intelligence (AI) has re-organized the ties between the individual, the State, and the private corporations. Modern states are becoming more dependent on algorithmic decision making, bio-metric recognition platforms, predictive analytics and mass data process systems. Such technological changes have heightened the issues of surveillance, commodification of data, and informational asymmetry. Personal information in this new digital ecosystem is no longer a transaction information, it is part of the identity and agency of individuals. As a result, privacy issues have blazed right into the areas of autonomy, dignity, and constitutional liberty.

This principle was first presented in the 1983 Census decision of the German Federal Constitutional Court, which promulgated the so-called informational self-determination, emphasizing that people must have the right to control the disclosure and use of their personal data.¹ In India, the same issue became urgent with the growth of the digital governance programs and biometric identity systems, leading to the fundamental constitutional issues associated with the extent of individual freedom in accordance with Article 21 of the Constitution.

The paradigm shift in the constitutionalization of privacy in India was a shift of narrow common-law approach towards a well-built rights framework. In a time when the AI systems are profiling and forecasting human behavior and shaping it, the question of digital autonomy protection requires a new constitutional review. Informational power is now becoming invisibly algorithmic power that flouts

¹ Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Dec. 15, 1983, 65

Entscheidungen des Bundesverfassungsgerichts [BVerfGE] 1 (Census Act Case).



traditional doctrines which are based on physical encroachment or direct action by the State.

1.2 History of the Development of the Privacy as a Fundamental Right in India

The history of the jurisprudence of privacy in India indicates a progressive yet resolute shift in the doctrine. In *M.P. Sharma v. Satish Chandra*², the Supreme Court adopted a narrow interpretative view by refusing to acknowledge an underlying right to privacy in the Constitution. Similarly, in *Kharak Singh v. State of Uttar Pradesh*³, the majority opinion, repudiated privacy as a separate constitutional protection even though Justice Subba Rao had made an early normative effort to view personal liberty as including privacy rights.

The judicial developments increased the scope of Article 21 especially in the case of *Maneka Gandhi v. Union of India*⁴, introducing substantive due process into the Indian constitutional law. Such interpretative change allowed the Court to assign dignity, fairness and reasonableness to the protection of life and personal liberty. Finally, a nine-judge Bench of Justice K.S. Puttaswamy (Retd.) v. Union of India⁵, well established that the right to privacy is a fundamental right that was guaranteed by the constitution in Article 21. The Court identified informational privacy as an essential element of dignity and autonomy, therefore entrenching the informational self-determination in the Indian constitutional framework.

The normative basis of exploring digital autonomy in the era of artificial intelligence is set through this jurisprudential development.

2. OBJECTIVES OF THE STUDY

The primary objective of this study is to critically analyze the constitutional underpinnings of the digital autonomy and informational self-determination in Article 21 of the Constitution of India. It attempts to examine how the identification of privacy by the Supreme Court in *Justice K.S. Puttaswamy (Retd.) v. Union of India*⁶ can be extended dogmatically to deal with new challenges that artificial intelligence and algorithmic governance bring.

The paper also seeks to determine whether the current legal provisions are sufficient to defend people against AI-driven profiling, automated decision-making, and mass data processing. It also evaluates whether the Digital Personal Data Protection Act, 2023⁷, is compatible with the constitutional principles of dignity, proportionality and accountability.

This research aims to introduce a rights-based constitutional design, enhancing informational control and transparency and institutional protection through artificial intelligence. The study takes a comparative approach to make normative conclusions about jurisdictions that have established more advanced systems of data protection, in particular, the General Data Protection Regulation (GDPR) of the European Union.⁸

3. LITERATURE REVIEW

3.1 Theoretical Literature Privacy and Autonomy

Privacy and autonomy conceptual relationship has dominated the center of liberal constitutional theory. Alan Westin's seminal works conceptualized the idea of privacy as an entitlement of individuals to decide when, how and in what extent information about them is disclosed to other persons and as a result, privacy is

² *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300.

³ *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.

⁴ *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.

⁵ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

⁶ *Ibid.*

⁷ The Digital Personal Data Protection Act, 2023 (No. 22 of 2023) (India).

⁸ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1.



viewed as a prerequisite to the development of dignity and self-determination.⁹ In the European context, the Census ruling of the German Federal Constitutional Court constitutionalized the doctrine of informational self-determination, where the individual control of personal information is key to the development of human personality, and the data aggregation and algorithmic profiling pose a risk to those conditions.¹⁰

3.2 Constitutional Privacy Jurisprudence of India

The use of privacy was at first derived beside personal liberty in the Indian constitutional scholarship especially with the growth of Article 21 in *Maneka Gandhi v. Union of India*.¹¹ It was however decisively resolved that the landscape of doctrine was in *Justice K.S. Puttaswamy (Retd.) v. Union of India*,¹² in which the court of nine judges asserted privacy as a fundamental right based on dignity, liberty and autonomy. Scholars have cited that although the judgment is a strong articulation of normative underpinnings of privacy, it does not provide a certainty of how technology is to be regulated and how algorithms are to be made.

3.3 Scholarship on AI and Human Rights around the World

With the recent rise in artificial intelligence, vast amounts of academic research have been produced on the issue of compatibility between the norms of human rights and algorithmic systems. The commodification of personal information and predictive behavior of markets in the digital marketplace is highlighted in the theory of surveillance capitalism by Shoshana Zuboff.¹³ It has been followed by other international publications, such as the Recommendation on the Ethics of Artificial Intelligence (UNESCO, 2021), which highlights the importance of transparency,

accountability, and human control of the automated mechanisms.¹⁴

3.4 Gaps in Existing Literature

Irrespective of the massive theoretical and comparative scholarship, the gaps are still abound. To begin with, the importance of incorporating informational self-determination and using it in relation to Article 21 in the context of AI governance has received limited focus. Second, Indian scholarship has not sufficiently defined the digital autonomy as a separate constitutional principle, other than privacy. Lastly, the lack of doctrinal comprehension of the way proportionality and dignity-based reasoning can guide AI regulation is evident. This paper aims to fill these gaps by integrating constitutional theory, comparative jurisprudence, governance frameworks and AI governance frameworks.

4. RESEARCH METHODOLOGY

4.1 Nature of Research

The research is a doctrinal and analytical study on the constitution. It mainly focuses on the meaning of Article 21 of the Constitution of India to determine the extent of informational self-determination and digital autonomy as generated in artificial intelligence. The study is normative in nature because it is aimed at not only describing the current legal principles, but also evaluating the suitability of the norms to deal with the new technological issues.

4.2 Research Design

The study is qualitative in format and it is organized in constitutional understanding and rights-based examination. It is a critical approach to judicial reasoning, especially to the privacy jurisprudence concluded with *Justice K.S. Puttaswamy (Retd.) v.*

⁹ Alan F. Westin, *Privacy and Freedom* (Atheneum, New York, 1967).

¹⁰ Bundesverfassungsgericht [BVerfG] Dec. 15, 1983, 65 BVerfGE 1 (Census Act Case).

¹¹ *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.

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

¹³ Shoshana Zuboff, *The Age of Surveillance Capitalism* (PublicAffairs, New York, 2019).

¹⁴ UNESCO, Recommendation on the Ethics of Artificial Intelligence (adopted 23 November 2021).



Union of India¹⁵, to establish the viability of its doctrinal base to include AI-driven models of governance. The design incorporates the theory of law with modern technology advancements to consider the structural risks by the use of algorithmic systems.

4.3 Sources of Data

The research is solely based on secondary sources. The major legal sources are the constitutional provisions, laws, like Digital Personal Data Protection Act, 2023¹⁶, and decisions of the Supreme Court of India. The sources used as the categories of secondary sources include peer-reviewed journal articles, scholarly books, comparative constitutional materials, and international instruments on data protection and AI ethics. The global regulatory trends are also put into context by consulting the authoritative policy reports and documents issued by international organizations.

4.4 Comparative Method

The developments in jurisdictions which have previously acknowledged informational self-determination are analyzed using a limited comparative approach, which is mainly Germany and the European Union. The aim is to attract normative views as opposed to importing alien teachings.

4.5 Analytical Framework

The normative approach is based on dignity-based constitutionalism and the proportionality criterion that is presented in Puttaswamy. It considers AI regulation in terms of the legality, necessity, proportionality, and process protection tests, thus aligning AI regulation with constitutional morality and individual autonomy.

5. CONCEPTUAL FOUNDATIONS: DIGITAL AUTONOMY AND INFORMATIONAL SELF-DETERMINATION

5.1 Connotation and Aspects of Digital Autonomy

Digital autonomy is the ability of people to have the meaningful control over their personal information, the digital identity, and the algorithmically mediated decision-making. It goes beyond the customary sense of privacy as secrecy and would rather include decisional independence, control over information and safeguard against behavioral manipulation. In the modern digital ecosystems, AI systems gather, deduce and forecast personal characteristics by constantly mining data. These systems determine the availability of credit, jobs, government services and even political information. Digital independence thus simply means non-invasion rather than non-algorithms domination. It requires visibility, responsibility and maintenance of personal agency in the data driven worlds.

5.2 Informational Self-Determination: Theoretical Basis and Origins

Informational self-determination became a doctrine that was brought to the fore in German constitutional jurisprudence. The German Federal Constitutional Court in its historic Census ruling of 1983, declared that the general right of personality encompassed in the basic Law encompasses the power of individuals to decide on how their personal data was collected and used, which resulted in bad blood of democratic participation and personality development.¹⁷ The informational self-determination was thereby put in perspective as not only data protection but as structural protection of human dignity and democratic order.

This doctrine is based on a theoretical context of the Kantian concept of autonomy in which individuals should be regarded as ends and not a subject of state or market actions. In the era of cyber technology when

¹⁵ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

¹⁶ The Digital Personal Data Protection Act, 2023 (No. 22 of 2023) (India).

¹⁷ Bundesverfassungsgericht [BVerfG] Dec. 15, 1983, 65 BVerfGE 1 (Census Act Case).



individuals are diminished to the status of predictable profiles by the profiling of their data, the applicability of this doctrine has magnified. It gives a criterion of rejecting mass surveillance and algorithmic control that obliterates the individual definition of self.

5.3 Correlation between Privacy, Dignity and Autonomy.

The values of privacy, dignity, and autonomy are mutually supportive of one another. It is in the Supreme Court of India, Justice K.S. Puttaswamy (Retd.). v. Union of India, affirmed that privacy is inherent to life and personal freedom in Article 21 and the same is pegged on human dignity.¹⁸ Losing control over the personal information, one can be profiled, typified, and bound in a way that disrupts their freedom of choice. Therefore, the normative link between dignity and autonomy is privacy.

5.4 Data as a Continuation of Personality

Individual information is becoming a continuation of personality in digitally networked societies. The digital personhood is formed by bio metrics identifiers, behavioral information and online engagement. The identity of the person is prone to manipulation and commodification when such data is aggregated and processed without any significant safeguards. Appreciating the fact that data is a continuation of personality makes the argument on informational self-determination not just policy providing regulation but a constitutional mandate, based on dignity and liberty.

6. ARTICLE 21 AND CONSTITUTIONALIZING DIGITAL PRIVACY IN INDIA

6.1 Expanding Interpretation of Article 21

Article 21 of the constitution of India asserts that no man shall be denied his right to life or his personal liberty without due process of law enacted under law.

¹⁸ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

¹⁹ Maneka Gandhi v. Union of India, (1978) 1 SCC 248.

²⁰ M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.

It was first construed limitedly, but much broader after Maneka Gandhi v. Union of India, in which the Supreme Court stated that procedure provided under Article 21 must be just, fair and reasonable¹⁹, this interpretive change brought the element of substantive due process to the Indian constitutional jurisprudence, and allowed the Court to encompass various unenumerated rights in the domain of life and personal freedom. Gradually, dignity, autonomy and personal choice were interpreted into Article 21 thus establishing the foundation on the acknowledgement of privacy as a constitutional guarantee. The development of Article 21 therefore changed it into a dynamic provision that can adapt to changing social and technological realities.

6.2 Judicial Recognition of Privacy

Among the laws addressing privacy concerns are the laws of many countries and states that have provided explicit legal protections regarding their citizens and their privacy rights.

The legal process to define privacy as one of the basic rights was a slow one. Far reaching rulings like M.P. Sharma v. Satish Chandra²⁰ and Kharak Singh v. State of Uttar Pradesh²¹ refused to accept privacy as a right of the constitution. But later decisions gradually recognized privacy interest in a particular setting. This was the final intervention by a nine-judge Bench in Justice K.S. Puttaswamy (Retd.). v. Union of India²² the Court constitutionalized Article 21. The Court acknowledged right to privacy by establishing that privacy is inherent in life and entailed as far as personal liberty is concerned, thus invalidating earlier judgments that would have restricted privacy.

6.3 Informational Privacy as Article 21 Facet

In case of Puttaswamy, the Court made it clear that informational privacy is a fundamental element of a right to privacy. Recognizing that the technological progress allows the State and non-State actors to

²¹ Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.

²² Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.



gather, store, and process enormous amounts of personal data which is the threat to individual autonomy, the Court made it clear that any such restriction should pass the test of legality, legitimate aim, proportionality, and procedural safeguards. This ideology offers the constitutional foundation of gauging AI-based surveillance and data controls.

6.4 Dignity, Technological Governance, and Constitution Morality

The constitutionalization of digital privacy is based on the larger desire to commit to constitutional morality and human dignity. Article 21 is now functioning more as a normative check to technological governance in order to make sure that innovation does not override the fundamental rights. Since citizenship and accessibility of services through digital infrastructures become more mediated, the constitutional questioning becomes essential to avoid arbitrary or disproportionate violations of the informational autonomy. This changing jurisprudence according to Article 21 places the digital privacy in the border of dignity, democracy, and responsible technological authority.

7. ARTIFICIAL INTELLIGENCE AND HOW INFORMATIONAL POWER IS CHANGING

7.1 Character and Construction of AI Systems

Artificial intelligence systems are machine learning algorithms that are trained on massive datasets to recognize the patterns to make predictive outputs. These systems are based on probabilistic modelling and iteration, as contrasted to deterministic software. Their design normally involves collection of data, training of the model, its validation, and deployment processes. The lack of transparency in these systems, or as it is occasionally termed as the black box

phenomenon, brings up the question of explainability and accountability.²³ As AI systems begin to control access to the labor market, credit, health care and state services, as well as provide the final decision-making power of the computerized workflow.²⁴

7.2 Algorithmic Decision-Making and Profiling

Predictive analytics used in algorithmic decision-making is automated classification and scoring. Profiling methods provide assumptions regarding behavior, preferences and risks of people. Although such systems are claimed to be efficient, they can recreate historical bias in training data.²⁵ The European Union General Data Protection Regulation (GDPR) explicitly acknowledges the risks related to automated decision-making and offers protection, one of which is the right not to be subject to the decisions made with the help of automated processing only.²⁶

7.3 Behavioral Manipulation, Surveillance Capitalism, and Big Data

Contemporary AI ecosystem is of close association with data-driven economic models. Shoshana Zuboff describes this type of paradigm as a form of surveillance capitalism, where human data is mined and sold to predict and push behaviors, which possibly alters the way democracies deliberate.²⁷ Commodification of personal experience disputes the conventional concept of consent and informational control.

7.4 Automated State Surveillance and Governance

States are now using AI in welfare management, preemptive policing, and biometric identification systems. Proportionality and due process come into question with such deployments, especially where automated systems are involved in the process of governing fundamental rights.²⁸ The chilling and the

²³ Frank Pasquale, *The Black Box Society* (Harvard University Press, 2015).

²⁴ Kate Crawford, *Atlas of AI* (Yale University Press, 2021).

²⁵ Solon Barocas & Andrew D. Selbst, "Big Data's Disparate Impact" (2016) 104 California Law Review 671.

²⁶ Regulation (EU) 2016/679 (General Data Protection Regulation), Art. 22.

²⁷ Shoshana Zuboff, *The Age of Surveillance Capitalism* (PublicAffairs, 2019).

²⁸ United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/39/29 (2018).



mass surveillance effect would be the reason that the constitutional protection of technologies should be introduced in the sphere of governance.

7.5 Data Exploitation and Power on the platform of the Private Sector

There is a high level of control of data infrastructures and algorithmic curation by digital platforms. Their dominance does not only generate structural informational power but it can shape economic and political behavior²⁹, thus regulatory responses should not focus only on the State surveillance but also on concentrated power in the hands of a few in digital markets.

8. NEW MENACES TO DIGITAL AUTONOMY IN THE AI ERA

8.1 Algorithmic Bias and Discrimination

The AI systems that are trained using past data tend to reproduce and enhance the existing social disparities. The term algorithmic bias refers to the unfairness of predictive models based on the disadvantages of certain groups of individuals resulting from biased training data, or undesirable design decisions. By means of such structural bias, opportunities are limited according to non-transparent assessments of computation, equality is compromised, and digital autonomy is violated. In the cases when people cannot comprehend or oppose algorithmic categories, autonomy is dominated by statistical inference.

8.2 Social Scoring and Predictive Policing Social Scoring

Predictive policing is based on the past crime data that is used to predict future criminal behavior. Although promoted as efficiency-promoting measures, these systems may increase the effects of policing marginalized populations since the use of data-driven

suspicion reshapes the presumption of innocence, making people the targets of surveillance due to probable conduct.³⁰ Equally, social scoring systems where a collective body of behavioral data is employed to score the trustworthiness of individuals also create significant constitutional issues. These systems are able to precondition the entry into the services and opportunities on a basis of algorithmically produced reputational measures, restricting free choice and democratic engagement.

8.3 Facial recognition and Mass Surveillance

Real-time identification of people in both the public and private areas can be achieved using facial recognition technologies. Research has revealed that these systems are more prone to women and people of colour, escalating the chances of incorrect identification.³¹ In addition to the issue of accuracy, the adoption of facial recognition on the platforms of mass surveillance systems has systemic risks on anonymity and freedom of assembly. The chilling effects of the normalization of biometric monitoring prevent people to exercise the fundamental freedoms. Such technologies have to be carefully reviewed against necessities and proportionality criteria in constitutional democracies.

8.4 Deepfakes and Informational Manipulation

Generative AI has made it possible to generate extremely realistic synthetic media, otherwise known as deepfakes. Deepfakes pose a risk to the integrity of the reputation, elections, and the credibility of the information systems.³² They also suppress the control that people have over their digital identity and the way they are portrayed online by creating a false reality.

8.5 Loss of Meaningful Consent in AI Ecosystems

The current AI systems are based on ubiquitous data scraping as a part of daily online communications.

²⁹ Lina M. Khan, "Amazon's Antitrust Paradox" (2017) 126 Yale Law Journal 710.

³⁰ Andrew Guthrie Ferguson, *The Rise of Big Data Policing* (New York University Press, 2017).

³¹ Joy Buolamwini & Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial

Gender Classification" (2018) 81 Proceedings of Machine Learning Research 1.

³² Danielle Keats Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security" (2019) 107 California Law Review 1753.



Long privacy policies and convoluted data-sharing conditions make consent more or less symbolic than substantive.³³ Constant tracking, behavioral analytics and cross-platform data integration reduces the ability of the users to make informed choice. Consequently, informational self-determination will be in danger of being a simulation, and a deeper structural protection is required rather than consent-based approaches.

9. INFORMATIONAL SELF-DETERMINATION COMPARED TO CONSTITUTIONAL PERSPECTIVE

9.1 Germany - Informational Self-Determination Doctrine

Information privacy Informational self-determination has taken its modern form in German constitutional jurisprudence. The German Federal Constitutional Court made the most famous Census declaration in 1983, when it declared that the general right of personality in Articles 1 and 2 of the allows persons to have the right to determine how their personal data are to be disclosed and used, as this would not lead to a chilling effect on personality development and democratic participation.³⁴ Informational self-determination was therefore not only defined as a privacy interest but a structural protection that was necessary in constitutional democracy. The technique has been strengthened by later German jurisprudence and the measures to data-processing have become subject to a severe review of proportionality and underline informational transparency and limited purpose.

9.2 GDPR and Data Sovereignty - European Union

On a supranational level, data protection has been institutionalized by the European Union as a fundamental right in the Charter of Fundamental Rights of the European Union, under Article 8.³⁵ This is operationalized in the form of the General Data

Protection Regulation (GDPR) which creates a duty of lawful processing, data minimization, limitation of purposes and accountability.³⁶ The GDPR is a regulatory paradigm based on data sovereignty and personal control, as well as firm supervisory bodies and transnational enforcement procedures. This rights approach to the protection of personal data considers it as part of human dignity and democratic governance.

9.3 United States: Sectoral Privacy Model

On the contrary, the United States is a sectoral and market-based privacy regulator. Instead of integrating an expansive constitutional principle of informational self-determination, the U.S. law system has legislated specific protections against unreasonable searches and seizures upon the fourth amendment, which is mostly limited to the restraint of the state.³⁷ The lack of a general federal information protection law has created a situation in which privacy issues are regulated individually by statute across small sectors, including health and finance.

9.4 Comparative Lessons for India

Constitutional philosophies are different through comparative analysis. Germany and the EU follow the models of dignity that focus on the structural restrictions of data power, and the U.S. model is focused on market elasticity and the industry-focused protection. The comparison experience would indicate that more than procedural consent mechanisms are needed to protect digital autonomy in the case of India. A stronger structure based on dignity, proportionality, and institutional responsibility such as the German and EU models can be much more aligned with the constitutional ethos of Article 21 and leave technological innovation to be accommodated.

³³ Daniel J. Solove, "Privacy Self-Management and the Consent Dilemma" (2013) 126 Harvard Law Review 1880.

³⁴ Bundesverfassungsgericht [BVerfG] Dec. 15, 1983, 65 BVerfGE 1 (Census Act Case).

³⁵ Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 391, Art. 8.

³⁶ Regulation (EU) 2016/679 (General Data Protection Regulation).

³⁷ Katz v. United States, 389 U.S. 347 (1967).



10. CONCLUSION

The change in the informational power in the era of artificial intelligence requires the reevaluation of the constitutional guarantees in Article 21 of the Constitution of India. The acknowledgment of the right to privacy as the right to fundamental right in Justice K.S. Puttaswamy (Retd.) v. Union of India³⁸ was a turning point towards the dignity-based constitutionalism as informational self-determination was foundational to the value of life and personal liberty. Nevertheless, the emergence of algorithmic governance, predictive analytics, biometric surveillance, and market forms based on data introduces issues that cannot be viewed within the traditional privacy paradigms.

Digital autonomy should develop as a substantive constitutional value that is able to respond to structural asymmetries that the AI systems generate. The consent-based models cannot be used in the conditions of the opaque environment, massive data aggregation, and behavioral control. Proportionality, transparency, and institutional accountability in governing informational power have proven to be critical elements of regulation that has gone through comparative constitutional experience, especially of Germany and the European Union.

In the end, the protection of digital autonomy needs to be balanced between the technological innovation and constitutional morality. The rights-based model of AI governance based on the principles of dignity, proportionality, and democratic control is crucial to make sure that technological advancement makes people feel empowered and not suppressed by their freedom of choice.

Reference

1. Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Dec. 15, 1983, 65 Entscheidungen des Bundesverfassungsgerichts [BVerfGE] 1 (Census Act Case).
2. M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.
3. Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.
4. Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
5. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
6. The Digital Personal Data Protection Act, 2023 (No. 22 of 2023) (India).
7. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119).
8. Alan F. Westin, Privacy and Freedom (Atheneum, New York, 1967).
9. Shoshana Zuboff, The Age of Surveillance Capitalism (PublicAffairs, New York, 2019).
10. UNESCO, Recommendation on the Ethics of Artificial Intelligence (adopted 23 November 2021).
11. Frank Pasquale, The Black Box Society (Harvard University Press, 2015).
12. Kate Crawford, Atlas of AI (Yale University Press, 2021).
13. Solon Barocas & Andrew D. Selbst, "Big Data's Disparate Impact" (2016) 104 California Law Review 671.
14. Regulation (EU) 2016/679 (General Data Protection Regulation), Art. 22.
15. United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/39/29 (2018).
16. Lina M. Khan, "Amazon's Antitrust Paradox" (2017) 126 Yale Law Journal 710.
17. Andrew Guthrie Ferguson, The Rise of Big Data Policing (New York University Press, 2017).

³⁸ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.



18. Joy Buolamwini & Timnit Gebru, “Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification” (2018) 81 Proceedings of Machine Learning Research 1.
19. Danielle Keats Citron, “Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security” (2019) 107 California Law Review 1753.
20. Daniel J. Solove, “Privacy Self-Management and the Consent Dilemma” (2013) 126 Harvard Law Review 1880.
21. Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 391, Art. 8.
22. Katz v. United States, 389 U.S. 347 (1967).

