

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 4

2026

© 2026 International Journal of Law Management & Humanities

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to submission@ijlmh.com.

Artificial Intelligence and Protection of Individual Autonomy: Reassessing Privacy, Dignity and Personal Liberty under Article 21 of the Indian Constitution

SHIVAM JAISWAL* AND PREKSHA SINGH**

ABSTRACT

Artificial Intelligence has shifted the constitutional question away from the collection of personal data and towards the generation of new knowledge about individuals and its use to shape the environments in which they choose. Modern AI systems draw sensitive inferences from mundane data, assign persistent algorithmic identities, and personalise informational environments in ways that can influence preference formation without any prohibition, coercion or unauthorised disclosure. This paper asks whether, and on what basis, AI-driven inferential profiling and algorithmic personalised influence amount to an unwarranted encroachment on the right to decisional autonomy under Article 21 of the Indian Constitution. It traces the movement of Indian jurisprudence from the formal liberty of A.K. Gopalan to the substantive personal liberty of Maneka Gandhi, the dignity foundation laid in Francis Coralie Mullin, the privacy and informational self-determination reasoning of Puttaswamy, and the decisional-autonomy line running through Suchita Srivastava, NALSA, Shafin Jahan, Navtej Singh Johar and Joseph Shine. Drawing on a limited comparison with the European Union's data-protection and artificial-intelligence regimes, and on a critical assessment of the Digital Personal Data Protection Act, 2023 and the Information Technology Act, 2000, the paper argues that the existing framework protects informational privacy but not the cumulative transformation of data into inferential and behavioural power. It proposes algorithmic autonomy as a derivative interpretative principle rather than a new fundamental right, and sets out an Algorithmic Autonomy Proportionality Test structured around interference, constitutional attribution, legality, legitimate aim, necessity, proportionality in the strict sense, and procedural safeguards with effective remedies.

Keywords: *artificial intelligence, Article 21, informational privacy, human dignity, decisional autonomy, inferential profiling, algorithmic manipulation, informational self-determination, Digital Personal Data Protection Act 2023, proportionality*

* Author is an LL.M. Graduate at Department of Law, MJP Rohilkhand University, Bareilly, Uttar Pradesh, India.

** Author is an Assistant Professor at Department of Law, MJP Rohilkhand University, Bareilly, Uttar Pradesh, India.

I. INTRODUCTION

Artificial Intelligence, hereinafter referred to as AI, is transforming the context in which people enjoy their basic rights. Although the collection, storage and transmission of personal data are primarily the domain of traditional information technologies, modern AI systems can analyse vast and varied data sets, draw sensitive inferences, create predictive profiles, classify people, predict behavioural tendencies and personalise digital environments. These capabilities enable AI systems to move beyond mere knowledge of people to influence the informational and decision-making contexts in which they form choices and preferences. The constitutional issue that arises is not only one of informational privacy or unauthorised data processing. It extends to the protection of human dignity, personal freedom and autonomy of choice from technologically mediated profiling and influence.

Indian constitutional law has, over the years, become a more substantive body of rights, fundamental to human dignity and individual freedom, rather than a right to life and personal liberty that may be denied except through a procedure prescribed by law. The Supreme Court in its jurisprudence has recognised privacy as a part of life and personal liberty and has associated it closely with dignity, autonomy, informational self-determination and the freedom of the individual to make fundamental choices in life, culminating in the landmark judgment of *Justice K.S. Puttaswamy (Retd.) v. Union of India*.¹ Subsequent and concurrent constitutional decisions on sexual orientation, reproductive choice, gender identity, intimate association, marriage and personal relationships have reinforced the notion that the Constitution guarantees the right of individuals to be autonomous persons and to make important choices and decisions without unwarranted interference.

The new inferential profiling made possible by AI, however, raises a problem for the existing constitutional framework. The body of privacy jurisprudence has been largely shaped by the issues of surveillance, collection and disclosure of personal information, bodily intrusion, and direct restrictions on individual choice. The challenge posed by AI systems is a qualitatively different one. These systems can generate sensitive information about people that they never intended to give, assign them probabilistic identities, classify them according to their predicted characteristics or future actions, and organise information, opportunities and options for them by means of correlations, predictive analytics and machine-learning techniques. The act of choice can then be influenced by the ranking, targeting and optimisation processes in digital environments that are personalised but opaque to the people who are targeted.

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

The shift from data collection to inference, and from inference to behavioural influence, poses a constitutional challenge that remains unanswered: how is informational privacy to be safeguarded in an era of AI systems that not only gather information about individuals, but also generate new knowledge about them and use that knowledge to shape their decisional environments? Where this is the case, the constitutional injury may be suffered even if there is no unauthorised disclosure of personal information. Persistent profiling, sensitive inferences, the exploitation of individual vulnerabilities and highly personalised choice architectures can shape the conditions of preference formation and decision-making. AI therefore raises a question for constitutional law: can decisional autonomy be limited by indirect, cumulative and technologically mediated influences, rather than by direct prohibition or coercion?

The difficulty lies in the fact that many of the existing AI facilities are developed and operated by private companies. Digital platforms, technology firms, financial institutions, employers and other private actors increasingly use AI systems to classify individuals, determine who may be granted access to opportunities, tailor information, and influence behaviour. Traditionally, however, Article 21 is a protection against the State. The growing capacity of private AI systems to affect constitutionally protected interests then raises issues of the horizontal dimension of fundamental rights, the constitutional role of private actors in public or functionally significant roles, and the positive duties of the State to protect people from serious interference with their privacy, dignity and autonomy in the context of private algorithmic power.

The existing legal system in India is inadequate to deal with these issues. The Digital Personal Data Protection Act, 2023 regulates the processing of personal data in digital form and establishes obligations of data fiduciaries and rights of data principals.² This architecture is still mostly concerned with the processing of personal data, rather than with broader constitutional issues of inferences, predictive profiling, personalised influence and algorithmic manipulation. The Information Technology Act, 2000 was enacted before the emergence of modern AI tools and does not adopt a comprehensive rights-based approach to assessing interference with individual autonomy by AI.³ The evolving governance landscape of AI in India thus takes place against an important constitutional question: what do the constitutional rights to privacy, dignity and decisional autonomy mean in terms of legally enforceable standards that can address the unique nature of the power wielded by AI systems?

² Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023).

³ Information Technology Act, No. 21 of 2000, INDIA CODE (2000).

The issues of privacy, data protection, algorithmic discrimination, transparency, accountability and automated decision-making have been broadly discussed in the legal literature on AI. Inferential privacy studies have demonstrated that data-protection regimes can be ineffective at protecting individuals from sensitive inferences drawn through algorithmic analysis,⁴ while studies of algorithmic manipulation and recommender systems have demonstrated that personalised digital environments can affect human agency.^{5,6} These discussions are usually treated as individual regulatory issues, however. Indian constitutional law has yet to develop a clear doctrinal framework to determine when algorithmic inferences, profiling and personalised behavioural influence become a constitutionally relevant interference with the exercise of individual autonomy under Article 21. In the absence of such a framework, there are open questions about the extent of constitutional harm, who is responsible for the interference, how such interference is to be justified, and the process and protections needed to ensure that meaningful human agency remains.

Against this backdrop, the main research question that this paper seeks to answer is whether, and on what basis, AI-based inferential profiling and algorithmic personalised influence amount to an unwarranted encroachment on the right to decisional autonomy guaranteed by Article 21 of the Indian Constitution, and what constitutional framework should be used to evaluate such interference. The paper assumes that current fundamental-rights and data-protection regimes offer limited protection because they focus mainly on informational privacy and data processing, rather than on the cumulative transformation of personal data into inferential and behavioural power. It contends that Indian constitutional jurisprudence has the normative underpinnings to address these new harms but needs a more robust doctrinal structure to make sense of the concepts of privacy, dignity, informational self-determination and decisional autonomy in the context of AI-based profiling and influence.

This work explores the evolution of the constitutional concepts of privacy, dignity, informational self-determination and decisional autonomy, and their relevance to inferential profiling and behavioural influence by AI. The analysis is further complemented by a limited comparative study of the European Union's data-protection and artificial-intelligence regulatory

⁴ Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, 2019 COLUM. BUS. L. REV. 494, 494–620.

⁵ Daniel Susser, Beate Roessler & Helen Nissenbaum, *Technology, Autonomy, and Manipulation*, 8 INTERNET POL'Y REV., no. 2, 2019, at 1, 1–22.

⁶ Karen Yeung, *"Hypernudge": Big Data as a Mode of Regulation by Design*, 20 INFO., COMM'C'N & SOC'Y 118, 118–36 (2017).

regimes,^{7,8} not to suggest wholesale adoption of foreign regulatory models, but to look for legal principles and protections that are relevant to the evolution of Indian constitutional doctrine. The paper also critically assesses the Digital Personal Data Protection Act, 2023 and the Information Technology Act, 2000 to see whether the current legislation is sufficient to safeguard the constitutionally protected interests of the people affected by the use of AI systems. AI requires constitutional law to go beyond a purely informational understanding of privacy to one that can deal with algorithmic interference with the formation and exercise of individual choice. To build such a framework, the paper proposes to conceptualise algorithmic autonomy as a derivative constitutional principle based on the guarantees of privacy, dignity, informational self-determination, decisional autonomy and personal liberty provided by Article 21. Algorithmic autonomy is not offered as a new or stand-alone fundamental right. Instead, it offers a doctrinal approach to the use of current constitutional protections in situations where AI systems make sensitive inferences, create consequential profiles, personalise decisional environments, exploit vulnerabilities, or otherwise exercise technologically mediated influence over people.

II. CONSTITUTIONAL FOUNDATIONS OF INDIVIDUAL AUTONOMY UNDER ARTICLE 21

In India, the constitutional protection of individual autonomy has evolved from a procedural right into a substantive right based on liberty, dignity, privacy and autonomy of the individual. The Constitution does not explicitly state that there is a fundamental right to autonomy, but the Supreme Court of India has increasingly held that personal liberty protects not only against physical restraint but also against unwarranted interference in the formation of identity, the exercise of choice and the development of personality. This doctrinal development offers a constitutional lens through which to explore whether AI-based inferential profiling and technologically mediated influence may be legally recognised as interferences with personal liberty.

⁷ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

⁸ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence and Amending Certain Union Legislative Acts (Artificial Intelligence Act), 2024 O.J. (L 1689) 1.

A. From Physical Liberty to Substantive Personal Liberty

The initial reading of Article 21 was formal and compartmentalised, in the sense that fundamental rights were read as if they were separate categories of rights. In *A.K. Gopalan v. State of Madras*, the Supreme Court understood the meaning of “personal liberty” as freedom from physical restraint and considered the fundamental rights in Part III as separate constitutional rights operating in different spheres.⁹ In this way, deprivation of liberty was constitutionally acceptable if it was the result of a procedure established by a competent legislature, and was subject to minimal judicial scrutiny of the substantive fairness or reasonableness of the procedure.

The basic tenets of this limiting view were gradually undermined. In *R.C. Cooper v. Union of India*, the Supreme Court did not accept the notion that fundamental rights exist in separate compartments, and laid emphasis on the impact of State action on the protected rights and not only on the formal object of the legislation.¹⁰ This change in doctrine was pivotal in *Maneka Gandhi v. Union of India*, where the Court redefined the meaning of Article 21.¹¹ The Court ruled that any process which takes away the life or personal liberty of an individual must be “right, just and fair” and not arbitrary, fanciful or oppressive. Articles 14, 19 and 21 were seen as a triad of constitutional provisions, and State interference had to meet the tests of fairness, non-arbitrariness and reasonableness.

The importance of *Maneka Gandhi* goes beyond procedural due process. The wide interpretation allowed Article 21 to become a constitutional basis for a variety of substantive rights that are essential to a meaningful life.¹² The Court then acknowledged that the right to life is not merely the right to animal existence, but the right to live with dignity and individual freedom. This evolutionary nature is especially significant when it comes to artificial intelligence. AI-driven infringement of individual liberty can take many forms that do not resemble traditional physical restrictions or legal bans. The doctrinal evolution started by *Maneka Gandhi* allows Article 21 to react to such changes, as the constitutional definition of liberty is not limited to the forms of State interference that have been recognised historically.

B. Human Dignity as the Normative Foundation of Article 21

Human dignity is a key element of the substantive component of Article 21. In *Francis Coralie Mullin v. Administrator, Union Territory of Delhi*, the Supreme Court held that the right to life

⁹ *A.K. Gopalan v. State of Madras*, A.I.R. 1950 S.C. 27 (India).

¹⁰ *Rustom Cavasjee Cooper v. Union of India*, (1970) 1 S.C.C. 248 (India).

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

¹² *Maneka Gandhi*, (1978) 1 S.C.C. 248.

is also a right to live with human dignity and to the essentials for the complete development of the human personality.¹³ Dignity is thus not only a constitutional aspiration, but a principle that guides the extent of life and personal freedom.

Later, the issues of dignity and autonomy came to the fore in constitutional jurisprudence. Dignity is about recognising people as individuals who are able to make decisions, choose their relationships, define themselves and live their lives. Constitutional protection is compromised when people are treated as “objects of administration”, “categories of risk” or “tools for external goals” without taking into account their agency and individuality.

One of the unique dignity issues is the growing use of algorithmic systems to build probabilistic representations of people. People may be categorised on the basis of their anticipated actions, assumed tastes, credit rating, job ability, political views, susceptibility or dangerousness. Such classifications may affect the treatment and perception of people by governments and private institutions. The constitutional issue is not that all algorithmic classifications are inherently demeaning. Rather, the long-term and consequential use of machine-generated representations can reduce people to profiles based on data, which do not account for their potential for change, context and self-definition.¹⁴

The dignity jurisprudence of Article 21 thus serves as an important normative framework for assessing AI systems. The use of AI systems that create and apply algorithmic identities that have consequences should be subject to constitutional review, as dignity demands that people be recognised as constitutional persons, not objects of technological classification.

C. Privacy, Informational Self-Determination and Individual Autonomy

In *K.S. Puttaswamy v. Union of India*, the judgment gave the most detailed expression to the constitutional nexus between privacy and autonomy.¹⁵ A Bench of nine judges unanimously declared privacy a fundamental right enshrined in the Constitution and found its roots in dignity, liberty and autonomy. The judgment did not accept restricting privacy to physical space or to the right to be left alone, but saw privacy as having a broader meaning, encompassing bodily integrity, personal information, intimate decisions and the freedom to shape one's life.

Informational privacy is a key aspect of *Puttaswamy*. The collection, aggregation, processing and use of personal information in a data-driven society can lead to a significant power imbalance between individuals and institutions. Informational privacy is about an individual's

¹³ *Francis Coralie Mullin v. Administrator, Union Territory of Delhi*, (1981) 1 S.C.C. 608 (India).

¹⁴ Mireille Hildebrandt, *Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning*, 20 THEORETICAL INQUIRIES L. 83, 83–121 (2019).

¹⁵ *Puttaswamy*, (2017) 10 S.C.C. 1.

interest in controlling the dissemination and use of information about the self, and about the need for laws that can prevent unwanted intrusion and misuse.

The concept of informational self-determination, under which people have meaningful control over information about their lives, was also used in the judgment. The principle acknowledges that the free collection and use of personal data may affect the freedom of individuals even where no physical force is involved. If a person is constantly monitored or profiled, or is unsure how their personal information will be used, they may change their behaviour and lose their ability to act freely.

AI significantly complicates this constitutional structure. AI systems do not merely gather or use information that people give them willingly. They create new knowledge through correlations and forecasting. Sensitive attributes, preferences, vulnerabilities and behavioural tendencies can be deduced from seemingly unrelated data.¹⁶ A person can thus lose control of information about themselves even though they did not knowingly provide it.

This is an example of the shortcomings of a control-based theory of informational privacy. Constitutional protection may not apply to knowledge created algorithmically about individuals, if it is only about information provided or possessed by individuals. But the reasoning of *Puttaswamy* is more expansive. The judgment acknowledges that privacy safeguards the conditions that enable individual autonomy, and not only the privacy of data.¹⁷ Where algorithmically driven inferences have a significant impact on an individual's identity, opportunities or choices, they may therefore implicate Article 21, where they are likely to affect informational self-determination or where they create an unjustified power imbalance.¹⁸

D. Decisional Autonomy under Indian Jurisprudence

Decisional autonomy has been increasingly accepted as an integral part of dignity and personal freedom in Indian constitutional jurisprudence. In *Suchita Srivastava v. Chandigarh Administration*, the Supreme Court upheld the right of reproductive choice as a part of personal liberty under Article 21, and established the right of individuals to make intimate decisions about their bodies and reproductive lives.¹⁹

The Court in *National Legal Services Authority v. Union of India* equated dignity and autonomy with the right of the person to decide and express their gender identity.²⁰ The judgment affirmed

¹⁶ Wachter & Mittelstadt, *supra* note 4.

¹⁷ Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1904–33 (2013).

¹⁸ *Puttaswamy*, (2017) 10 S.C.C. 1.

¹⁹ *Suchita Srivastava v. Chandigarh Administration*, (2009) 9 S.C.C. 1 (India).

²⁰ *National Legal Services Authority v. Union of India*, (2014) 5 S.C.C. 438 (India).

that self-determination is a key element of personal autonomy, and that external categorisations that strip people of control over key aspects of their identity are wrong.

In *Shafin Jahan v. Asokan K.M.*, the Court reiterated that the right to choose a partner is a right of the individual and is an integral part of the right to liberty and dignity.²¹ The Court stressed that constitutional courts are not the place for the substitution of their judgment for the independent decisions of competent adults.

Likewise, in *Navtej Singh Johar v. Union of India*, the Court emphasised individual autonomy, dignity, privacy and constitutional morality as its core, and struck down the criminalisation of consensual same-sex relations.²² The judgment acknowledged that the right to self-determination in matters of identity, relationship and intimate decisions is protected by the Constitution, and that this right is not to be interfered with by the majority.

In *Joseph Shine v. Union of India*, the Court struck down the criminal offence of adultery and highlighted that the rights to dignity and autonomy are incompatible with legal frameworks that deprive people of equal moral agency and reduce them to the status of means to someone else's ends.²³

These decisions form a constitutional principle that goes beyond the protection of specific decisions. Article 21 guarantees the right of the individual as a distinct constitutional person with the ability to create an identity, form preferences and take important decisions about their way of life. Freedom from direct coercion and the maintenance of the conditions of meaningful choice are thus both essential to decisional autonomy.

E. The Constitutional Gap: From Protected Choice to the Conditions of Choice

This jurisprudence has some challenging questions to address in the context of AI-mediated environments. Algorithmic systems increasingly shape the information people are exposed to, the options they are given, the order in which options are presented, and the personalised stimuli that are used to shape behaviour. Such systems may be designed so as not to remove an option explicitly. However, they can still change the architecture of the choice-making and choice-exercising process. Where AI systems make inferences that affect major decisions, use sensitive inferences, engage in persistent profiling, or exploit personal vulnerabilities, the line between legitimate assistance and constitutionally relevant interference grows blurred.

²¹ *Shafin Jahan v. Asokan K.M.*, (2018) 16 S.C.C. 368 (India).

²² *Navtej Singh Johar v. Union of India*, (2018) 10 S.C.C. 1 (India).

²³ *Joseph Shine v. Union of India*, (2019) 3 S.C.C. 39 (India).

The constitutional law that has emerged, however, has been developed largely in the context of identifiable State action, direct restrictions on choice, surveillance, intrusion into the body, criminalisation, and the disclosure and collection of personal information. The autonomy issue raised by AI systems is a different one, as such systems can affect autonomy indirectly through inference, prediction, personalisation and the ongoing structuring of decisional environments.

III. AI-DRIVEN INFERENTIAL PROFILING AS A CONSTITUTIONAL CHALLENGE

AI has changed the definition of informational power by creating knowledge about people that goes beyond what they have given directly. Modern AI systems can process data such as behavioural patterns, digital interactions, transaction histories, location data and social connections to make inferences about a person's traits, preferences, vulnerabilities and likely behaviour. The constitutional significance of this ability lies in the difference between information about a person and the creation of new knowledge about that person. Indian privacy jurisprudence and data-protection law focus on the collection, processing and use of personal data, but AI-driven inferential profiling poses the question whether Article 21 protects people against consequential algorithmic representations and predictions that they did not disclose and did not meaningfully control.

A. Personal Data to Algorithmically Inferred Knowledge

There may be a legal difference between observed, derived and inferred data. Observed data are data that are directly provided by individuals or captured from their actions, such as transactions, searches, communications or online interactions. Derived data are data that are processed or compiled from other data. Inferred data, on the other hand, are conclusions reached through algorithmic analysis about characteristics, preferences, vulnerabilities or likely behaviour.²⁴

The difference is of constitutional significance, as AI systems can draw highly sensitive inferences from seemingly mundane data. Online behaviour can be used to infer political or religious affiliations, buying habits or health issues; mobility data can be used to infer financial status; and patterns of interaction can be used to predict psychological traits or future behaviour. People can then become the object of kinds of knowledge production of which they have no awareness.²⁵

The fact that algorithmically generated knowledge about a person is inferred rather than collected should not mean that it escapes constitutional scrutiny where it is sufficiently sensitive

²⁴ Wachter & Mittelstadt, *supra* note 4.

²⁵ Hildebrandt, *supra* note 14.

or consequential to affect protected interests. A technologically neutral understanding of Article 21 must take into account the impact of information processing on the person, and not just the source of the information.

B. Inferential Profiling and the Limits of Informational Self-Determination

Informational self-determination is based on the idea that people should have some control over information about themselves. That premise is undermined by AI-driven inference, which means that people cannot control information that they do not expect or understand. Consent to the processing of one type of personal data may lead to the drawing of significantly different and more sensitive conclusions.²⁶

This leaves a space between formal control of data and substantive control of the production of personal knowledge. A person may agree to the gathering of browsing data without reasonably expecting it to be used to determine their political leanings, emotional state or financial problems. Likewise, the removal or correction of underlying personal data does not necessarily mean that profiles and predictions previously created from that data are removed or corrected.

The legal challenge is not limited to informational secrecy. Inferential profiling shifts the balance of power away from individuals and towards entities that can analyse large data sets. The capacity to produce knowledge about persons without their meaningful involvement can lead to an informational imbalance that can affect autonomy even where formal requirements of notice and consent have been met.²⁷

Article 21 should therefore be read to shield people not only from the unjustified collection of personal data, but also from highly intrusive or impactful algorithmic knowledge production. This protection does not preclude every inference. Prediction and classification are key components of many AI applications that are beneficial to society. Where the sensitivity, purpose, opacity or consequences of inferred information substantially interfere with privacy, dignity and autonomy, constitutional scrutiny is required.

C. Algorithmic Profiling and the Construction of Algorithmic Identity

Inferential profiling is especially significant where algorithmically derived inferences are used to build a persistent representation of a person. AI systems are increasingly used to classify people according to their predicted preferences, risk, creditworthiness, employability,

²⁶ Wachter & Mittelstadt, *supra* note 4.

²⁷ FRANK PASQUALE, *THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION* (Harvard Univ. Press 2015).

vulnerability and behavioural tendencies. These representations can then affect the opportunities, information, services and treatment that people receive.²⁸

There is no violation of Article 21 merely because an algorithmic profile exists. The constitutional issue is raised when such profiles are intrusive or significant enough to affect dignity, opportunity, reputation or meaningful choice. The legal inquiry should therefore explore the sensitivity of the inference, the purpose for which the profile is developed, the consequences of using the profile, the level of opacity, and the capacity of the individual to question the accuracy or relevance of the profile.²⁹

D. Private Algorithmic Power and Constitutional Responsibility

Inferential profiling is further complicated by the fact that many AI systems are run by private companies. Digital platforms, employers, financial institutions, insurers and technology companies have vast abilities to create profiles and predictions about people.^{30,31} The traditional vertical approach to fundamental rights poses problems when interference with privacy or autonomy is not direct, but is instead brought about by private technological means.

The State is not necessarily relieved of constitutional obligations simply because it uses private vendors to provide algorithmic systems, or because it uses machine-generated profiles created outside the State's institutions. If public authorities rely on AI-generated inferences to decide who is eligible for benefits, who is targeted by the police, who gets a job, who gets an education, or who has access to other substantial interests, constitutional review should be directed at the informational processes on which governmental decisions are based.

The question is whether the State also has a positive obligation to control private inferential power where it is likely to have a serious impact on constitutional autonomy.³² Where the initial interference comes from a private party, effective protection of informational privacy and individual self-determination may require the State to put in place safeguards in relation to intrusive profiling, sensitive inferences, contestability and remedies.

²⁸ Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 1–33 (2014).

²⁹ Andrew D. Selbst & Solon Barocas, *The Intuitive Appeal of Explainable Machines*, 87 FORDHAM L. REV. 1085, 1085–1139 (2018).

³⁰ Jack M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. DAVIS L. REV. 1149, 1149–1210 (2018).

³¹ JULIE E. COHEN, *BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM* (Oxford Univ. Press 2019).

³² Stephen Gardbaum, *The “Horizontal Effect” of Constitutional Rights*, 102 MICH. L. REV. 387, 387–459 (2003).

IV. AI-MEDIATED MANIPULATION AND THE CONSTITUTIONAL PROTECTION OF DECISIONAL AUTONOMY

The constitutional considerations raised by AI are not limited to the creation of sensitive inferences and algorithmic profiles. Inferential profiling has its greatest significance in its ability to support increasingly personalised methods of influence that can affect the context in which people decide what to do. AI systems are no longer just about managing information; they also shape what information people see, how it is organised, what options are presented, if any, and the tailored inputs that will influence future behaviour. Recommendation engines, targeted advertising systems, predictive analytics and generative AI applications constantly monitor and adapt to each user's preferences and behaviour, creating an ever-changing informational landscape designed to maximise engagement, persuasion or business results. These systems do not typically make decisions for their users, but they are beginning to have the capacity to shape preferences and decision-making processes in more subtle ways. This is a new constitutional challenge, as Article 21 protects not only the freedom to make choices, but also the autonomy that makes those choices meaningful.

Indian constitutional jurisprudence has always given due emphasis to the fact that autonomy is linked with dignity and personal liberty. Relationships and reproductive decisions, as well as identity, belief and lifestyle choices, have consistently been defined as part of a protected zone of personal autonomy. These choices rest on a constitutional principle that treats people as the primary authors of their lives, free from undue outside intervention in areas affecting their personality and self-development. A much subtler, yet impactful, mode of interference is added by AI-based systems. They do not set out to tell people what they can and cannot do; rather, they shape them through constant personalisation, behavioural prediction and algorithmic optimisation.

The difference between persuasion and constitutionally significant manipulation is thus a crucial one to consider. In a democratic society, diverse forms of persuasion are accepted as a regular part of life, such as commercial campaigns, political communication and public awareness campaigns. Typically, these practices assume that people are capable of paying attention and making informed choices between conflicting sources of information. AI-driven systems differ in that they are designed with a large amount of behavioural data, predictive analytics and continuous feedback mechanisms that allow them to detect individual vulnerabilities and tailor influence at a level of specificity not previously possible.³³ The aim is

³³ Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 995–1051 (2014).

not only to send a message, but to maximise the chances of delivering the right message, recommendation or opportunity in order to maximise the behavioural impact on a specific person.

The constitutional problem with algorithmic choice architecture arises where it has a material effect which substantially undermines the conditions that enable an independent decision.³⁴ Long-term personalisation, emotional targeting, the exploitation of cognitive biases and repetitive behavioural reinforcement can, over time, influence perceptions, preferences and choices in ways over which the person may not feel they have control. Rather than the question whether these decisions are made by AI, the issue is whether AI may systematically affect the informational context in which constitutional autonomy is exercised. Freedom of choice becomes less real where the alternatives, the information about those alternatives, and the cues about what to do are continually arranged on the basis of predictive assessments directed at specific outcomes.

Historically, Article 21 has safeguarded people from direct compulsion by the State. Constitutional jurisprudence must acknowledge that liberty can be infringed by more subtle technological means that leave the impression of free choice while in fact significantly determining the circumstances in which the choice is made.³⁵ This is not to say that all algorithmic recommendation and personalisation is constitutionally problematic. AI systems have many positive social applications, such as making information more accessible, improving health care, and assisting in education, public administration and innovation. The intensity and consequences of algorithmic influence should thus be the subject of constitutional review, rather than the mere presence of AI-assisted decision-making. The sensitivity of the information inferred, the level of personalisation, the use of identifiable vulnerabilities, the lack of transparency in the decision-making process, the importance of the interests involved and the presence of alternatives that are meaningful to the individual all become relevant in determining whether the influence exerted by AI is an unjustified interference with decisional autonomy.

Current legislation offers only partial answers to these questions. Data-protection law is mainly concerned with the collection and processing of personal data, and consumer-protection law with deceptive or unfair commercial practices. Neither fully addresses the cumulative transformation of personal data into behavioural influence which can affect constitutionally protected autonomy. The constitutional issue is not just about controlling information

³⁴ Yeung, *supra* note 6.

³⁵ Susser, Roessler & Nissenbaum, *supra* note 5.

processing, but about determining when predictive technologies become tools that can have a real impact on the exercise of individual liberty.

The shift from inferential profiling to behavioural influence is a clear example of how AI converts informational power into behavioural power. Institutions with advanced AI capabilities are no longer just learning more about people; they are now able to predict, personalise and shape human behaviour through technologically mediated environments. To be relevant to modern threats to liberty, constitutional doctrine must acknowledge that meaningful autonomy requires not only that choices be made formally, but also that the conditions in which choices are made be preserved free from undue algorithmic influence. The current legal landscape, however, does not offer a clear answer to these new constitutional questions. It is therefore important to consider whether the existing regulatory framework in India, including the Digital Personal Data Protection Act, 2023 and other legal tools, is sufficient to safeguard individuals from interference with their decisional autonomy by AI.³⁶

V. WAY FORWARD: TOWARDS A CONSTITUTIONAL DOCTRINE OF ALGORITHMIC AUTONOMY UNDER ARTICLE 21

The above analysis shows that the constitutional challenge raised by AI goes beyond the gathering and processing of personal data. AI systems can be used to derive sensitive inferences, predictive profiles and personalised decisional environments from personal data, which can shape individual behaviour. This progression from information to inference, from inference to prediction, and from prediction to behavioural influence can have an impact on privacy, dignity and personal liberty without necessarily involving a legal prohibition or physical restraint. To be relevant to new technological forms of power, the guarantee of autonomy under Article 21 should cover the interference of AI with the conditions in which people make choices and form preferences.

Algorithmic autonomy can be defined as the right of the individual to maintain meaningful control over the development of their identity, preferences and important personal choices, free from unwarranted algorithmic inference, profiling and manipulation. It does not have to be declared a new fundamental right. Dignity, privacy, informational self-determination, decisional autonomy and personal liberty have been the consistent themes of Indian constitutional jurisprudence in the interpretation of Article 21. Algorithmic autonomy can therefore serve as an interpretative principle that applies these guarantees to the environments in which AI is used.

³⁶ Digital Personal Data Protection Act, *supra* note 2.

Such an approach already has doctrinal foundations. *Justice K.S. Puttaswamy (Retd.) v. Union of India* establishes the link between privacy, dignity, liberty and individual autonomy, and the Supreme Court's general autonomy jurisprudence protects the individual as a constitutional person who can make meaningful decisions about their life and identity.³⁷ AI poses challenges to these protections, as interference can happen prior to the final decision-making process. How preferences are formed, and how alternatives are perceived, can be affected by persistent profiling, predictive classification, personalised information environments and the exploitation of vulnerabilities. The protection of the formal availability of choice must therefore be extended to the protection of the conditions which are necessary for meaningful choice.

The recognition of algorithmic autonomy does not mean that all recommendations, classifications, predictions or personalised services infringe Article 21. There are many legitimate and beneficial uses of AI systems. The nature, intensity and effects of algorithmic influence should be sufficiently material to affect protected autonomy before constitutional scrutiny is triggered. It is thus essential to have a structured legal framework to differentiate between ordinary technological influence and interference which is constitutionally relevant.

An Algorithmic Autonomy Proportionality Test is suggested for this purpose. The first step is to decide whether the AI system creates a constitutionally relevant interference with individual autonomy. Factors to consider are the sensitivity of algorithmically generated inferences, the intensity and persistence of profiling, the level of personalisation, the exploitation of psychological, cognitive, economic or situational vulnerabilities, the importance of the interests involved, and the cumulative effects of long-term exposure to algorithmically structured environments. The importance of the system to human agency should be the basis for constitutional significance, not just whether people have the formal power to choose.

The second stage is constitutional attribution and responsibility. If AI systems are being used directly by public authorities, then the normal constitutional review process should apply. Governmental institutions should not be allowed to shift responsibility for algorithmic functions to private vendors, or to use privately created profiles in public decision-making. If there is significant interference from private AI systems, courts should consider whether the AI is used for public functions, or whether the circumstances give rise to positive obligations of the State to take reasonable measures to prevent serious and foreseeable interference with privacy, dignity and autonomy.

³⁷ *Puttaswamy*, (2017) 10 S.C.C. 1.

The third stage concerns legality. Governmental use of AI that significantly impinges on autonomy should have a clear, accessible and predictable legal basis. Administrative convenience, technological efficiency or the mere availability of AI cannot replace lawful authority. The fourth stage involves identifying a legitimate goal and a rational connection between the AI system used and that goal.

The fifth stage involves a review of necessity and of less restrictive alternatives. Courts and regulators should consider whether the legitimate goals could be met with less intrusive processing, less profiling, limitations on sensitive inferences, anonymisation, non-personalised systems, meaningful opt-out mechanisms, or human decision-making. The efficiency gains that can be achieved through extensive profiling should not by themselves be enough to make such profiling constitutionally permissible.

The sixth stage demands proportionality in the strict sense. The seriousness of the interference with privacy, dignity and decisional autonomy must be weighed against the importance of the legitimate objective. Some of the factors that should be taken into account are the sensitivity and reliability of algorithmic inferences, the degree of personalisation, the vulnerabilities exploited, the length of exposure, the consequences of algorithmic classifications, institutional power disparities, and the capacity of individuals to resist or leave the technological environment. AI systems that affect welfare, health, employment, education, financial access, policing or political participation should be subject to special attention.

Procedural safeguards and effective remedies are needed at the final stage. People can be unaware of being profiled, classified or personally influenced. Depending on the importance of the AI system, constitutional protections should include notice of consequential AI use, meaningful information about significant profiling and inferences, the possibility of challenging algorithmic representations that are inaccurate or unjust, meaningful human review, independent oversight, and effective judicial or administrative remedies.^{38,39} Transparency should not be a goal in itself but a means to empower people to comprehend and challenge technological power.

The proposed doctrine offers a way to extend Article 21 jurisprudence to new harms caused by AI without equating technological innovation with a violation of fundamental rights. It could be used to inform judicial review under Articles 32 and 226 in cases where governmental bodies use AI systems or algorithmic profiles in public decision-making. It can also guide legislative

³⁸ Margot E. Kaminski, *The Right to Explanation, Explained*, 34 BERKELEY TECH. L.J. 189, 189–218 (2019).

³⁹ Lilian Edwards & Michael Veale, *Slave to the Algorithm? Why a “Right to an Explanation” Is Probably Not the Remedy You Are Looking For*, 16 DUKE L. & TECH. REV. 18, 18–84 (2017).

and regulatory protections in relation to sensitive inferences, algorithmic impact assessments, vulnerable persons, human oversight, contestability and remedies.

The problem with Indian law is not, however, that it lacks constitutional principles that can address AI. Article 21 already guarantees privacy, dignity, informational self-determination, decisional autonomy and personal liberty. The challenge is that there is no clear doctrinal framework that can help to translate these protections into legal principles that can be applied to AI systems that infer, classify, predict, personalise and influence. The Digital Personal Data Protection Act, 2023 regulates the processing of digital personal data rather than specifically addressing the constitutional implications of inferential profiling and behavioural influence.⁴⁰ A rights-based constitutional approach is essential where AI systems have a material impact on human agency, and fragmented statutory and sectoral protections are not enough.

The constitutional challenge of AI therefore needs to shift from a focus on protecting people from informational intrusion to protecting them from the unjustified exercise of inferential and behavioural power. AI systems are increasingly turning data into knowledge, knowledge into prediction, and prediction into the ability to affect human behaviour. The doctrinal framework to address this transformation is algorithmic autonomy, which is based on the existing guarantees in Article 21 and calls for a structured review of constitutionally relevant uses of AI, according to the criteria of interference, attribution, legality, legitimate aim, necessity, proportionality, procedural safeguards and effective remedies.

The core constitutional issue with AI is not just the extent to which technological systems can know about people, but the extent to which institutions may be allowed to know, classify, predict and influence people. Article 21 has developed historically to safeguard dignity and liberty against new forms of power. It remains relevant in the era of AI, so long as people are not treated as mere objects of algorithmic prediction and behavioural optimisation. The constitutional commitment to personal liberty must therefore guarantee not only the right to make choices, but also the conditions that allow individuals to remain the meaningful authors of those choices.

⁴⁰ Digital Personal Data Protection Act, *supra* note 2.

VI. BIBLIOGRAPHY

1. *A.K. Gopalan v. State of Madras*, A.I.R. 1950 S.C. 27 (India).
2. *Rustom Cavasjee Cooper v. Union of India*, (1970) 1 S.C.C. 248 (India).
3. *Maneka Gandhi v. Union of India*, (1978) 1 S.C.C. 248 (India).
4. *Francis Coralie Mullin v. Administrator, Union Territory of Delhi*, (1981) 1 S.C.C. 608 (India).
5. *Suchita Srivastava v. Chandigarh Administration*, (2009) 9 S.C.C. 1 (India).
6. *National Legal Services Authority v. Union of India*, (2014) 5 S.C.C. 438 (India).
7. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).
8. *Shafin Jahan v. Asokan K.M.*, (2018) 16 S.C.C. 368 (India).
9. *Navtej Singh Johar v. Union of India*, (2018) 10 S.C.C. 1 (India).
10. *Joseph Shine v. Union of India*, (2019) 3 S.C.C. 39 (India).
11. *K.S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 S.C.C. 1 (India).
12. Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023).
13. Information Technology Act, No. 21 of 2000, INDIA CODE (2000).
14. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.
15. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence and Amending Certain Union Legislative Acts (Artificial Intelligence Act), 2024 O.J. (L 1689) 1.
16. Balkin, Jack M., *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. DAVIS L. REV. 1149, 1149–1210 (2018).
17. Calo, Ryan, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 995–1051 (2014).
18. Citron, Danielle Keats & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 1–33 (2014).
19. Cohen, Julie E., *What Privacy Is For*, 126 HARV. L. REV. 1904, 1904–33 (2013).

20. COHEN, JULIE E., *BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM* (Oxford Univ. Press 2019).
21. Edwards, Lilian & Michael Veale, *Slave to the Algorithm? Why a “Right to an Explanation” Is Probably Not the Remedy You Are Looking For*, 16 DUKE L. & TECH. REV. 18, 18–84 (2017).
22. Gardbaum, Stephen, *The “Horizontal Effect” of Constitutional Rights*, 102 MICH. L. REV. 387, 387–459 (2003).
23. Hildebrandt, Mireille, *Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning*, 20 THEORETICAL INQUIRIES L. 83, 83–121 (2019).
24. Kaminski, Margot E., *The Right to Explanation, Explained*, 34 BERKELEY TECH. L.J. 189, 189–218 (2019).
25. PASQUALE, FRANK, *THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION* (Harvard Univ. Press 2015).
26. Selbst, Andrew D. & Solon Barocas, *The Intuitive Appeal of Explainable Machines*, 87 FORDHAM L. REV. 1085, 1085–1139 (2018).
27. Susser, Daniel, Beate Roessler & Helen Nissenbaum, *Technology, Autonomy, and Manipulation*, 8 INTERNET POL'Y REV., no. 2, 2019, at 1, 1–22.
28. Wachter, Sandra & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, 2019 COLUM. BUS. L. REV. 494, 494–620.
29. Yeung, Karen, *“Hypernudge”: Big Data as a Mode of Regulation by Design*, 20 INFO., COMMUN & SOC'Y 118, 118–36 (2017).
