

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 2
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**



ARTIFICIAL INTELLIGENCE, SOCIAL MEDIA, AND PRIVACY RIGHTS: TRACING LEGAL AND SOCIETAL RESPONSES THROUGH A DOCTRINAL LENS

By *Bhanupriya*

Research Scholar from *MVN University,
Aurangabad, Haryana*

By *Dr. Rahul Varshney*

**Dean, School of Law, MVN University,
Aurangabad, Haryana**

ABSTRACT

The integration of the artificial intelligence (AI) into social media platforms has been a transformative step and has depicted how personal data is collected, inferred, monetised, and governed. Existing literature shows that algorithmic profiling, facial recognition, sentiment analysis, and targeted advertising have intensified data extraction beyond users' reasonable expectations, raising profound concerns for privacy and autonomy. This paper reviews how regulation has responded to these developments, mapping the historical trajectory from early data protection principles to contemporary AI governance. It examines pivotal legal and regulatory milestones such as the Information Technology Act, 2000; the Digital Personal Data Protection Act, 2023; and the other bills and laws that were discussed, alongside landmark privacy jurisprudence, including Justice K. S. Puttaswamy v. Union of India.

Adopting a doctrinal design, the study combines doctrinal legal analysis with studying the reports and data to understand the public perceptions of privacy and the ways users believe AI-driven social media hampers it through opaque profiling, behavioral manipulation, data permanence, and cross-platform

tracking. The research identifies gaps between formal legal safeguards and lived digital experiences, especially regarding consent, transparency, and algorithmic accountability.

By synthesizing legal analysis with user perspectives, the paper proposes a rights-centered framework for AI governance on social media that prioritizes explainability, purpose limitation, and meaningful consent. The study argues that without recalibrating privacy protections to address AI's inferential power, social media ecosystems risk normalizing pervasive surveillance under the guise of personalization.

Keywords: AI governance, social media, privacy rights, algorithmic profiling, consent, surveillance, data protection.

1. INTRODUCTION

The modern world is marked by an unprecedented growth of digital technologies, which have changed almost all spheres of human life. One such instrument is artificial intelligence, which has become a potent means of influencing the making of decisions across the industries such as healthcare, finance, education, governance, and law enforcement. India is and has been one of the largest digital economies in the world, and its digital infrastructure, internet penetration, and data creation have grown at a rapid rate in the last ten years. The transformation has not only provided new grounds for economic growth and efficient governance, but it has also posed new legal and ethical issues. The spread of AI and data-driven technologies has led to the massive collection, then processing, and, last, the storage of personal data.

The definition and legal meaning of privacy is "the right that determines the non-intervention of secret surveillance and the protection of an individual's information."¹ The right to privacy, in simple terms, means that a person shall not be subjected to unwanted

¹ The Law Dictionary, 'Privacy' (no date)
<https://thelawdictionary.org/privacy/>



publicity and that whatever data are disclosed according to the will of the person shall be kept confidential. Privacy encompasses the multiple dimensions, including privacy of information, bodily privacy, privacy of communications, and territorial privacy.

The term 'privacy' has changed its significance greatly in the last few years. Everyone has a natural instinct to safeguard their own privacy and dignity. Privacy may be understood from many angles in general, and it may have different interpretations depending upon the culture of each individual and location. Nowadays, everybody tries to safeguard their privacy owing to the increasing technology and usage of social networking sites. As Zuboff famously observed, the rise of surveillance capitalism has created a new economic logic in which human behaviour itself constitutes the raw material for prediction products traded in behavioural futures markets.² Nowhere is this economic logic more visible or more consequential for individual rights than on AI-powered social media platforms. Privacy is a multifaceted concept spanning personal, social, and technological dimensions³. Privacy issues in the digital age are primarily caused by the gathering, use, and sharing of personal information by a variety of organisations, including businesses, governments, and private citizens. Effective privacy protection strategies must strike a careful balance between the advantages of technology and individual rights. Since Western nations view privacy as a human right, privacy laws have been tightened worldwide to accommodate growing concerns about the security of personal data.

In order to gather, categorise, and profit from enormous amounts of personal data, social media companies like Meta, X (formerly Twitter), Instagram, YouTube, TikTok, and LinkedIn now use advanced AI architectures, machine-learning models, natural language processors, computer vision systems, and behavioural inference engines. The data extracted extends far beyond what users voluntarily share: AI systems infer sensitive attributes, including political beliefs, religious affiliations, sexual orientation, mental health conditions, and financial vulnerabilities, from seemingly innocuous behavioral signals.⁴ These inferences are systematically deployed for targeted advertising, content curation, and, as recent regulatory investigations have revealed, political micro-targeting.⁵

These advancements present a fundamental legal challenge: privacy rules intended for identified, limited data collection are unable to regulate probabilistic, inferential systems that operate at scale. India's constitutional recognition of the right to privacy as a fundamental right, per the nine-judge bench in *K.S. Puttaswamy v. Union of India*,⁶ was a watershed moment, yet the legislative architecture constructed in its aftermath, particularly the Digital Personal Data Protection Act, 2023, has already attracted scholarly critique for its governmental exemptions, its attenuated consent regime, and its silence on algorithmic accountability.⁷

The present work is engaged in a doctrinal study of the legal and social reactions to the phenomenon of AI-enabled privacy invasion on social media platforms.

² Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs, 2019) 8–11.

³ Mulligan D. K., Koopman C., Doty N. (2016). Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy. *Philos. Trans. R. Soc. Lond. A. Math. Phys. Eng. Sci.* 374:20160118. doi: 10.1098/rsta.2016.0118,

⁴ Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press, 2015) 3–6.

⁵ Yael Eisenstat, 'I Worked on Political Ads at Facebook.' 'Here's Why I'm Worried About the 2020 Election' (Washington Post, 4 October 2019).

⁶ *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (India).

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



The second section deals with an intellectual history of the concept of information self-determination and privacy rights. The third section involves analysis of the anatomy of AI-enabled data practices on social media platforms. Sections four and five provide a picture of Indian and comparative laws. The sixth section discusses judicial reactions. The seventh section highlights normative gaps in the system.

2. FROM DATA PROTECTION TO INFORMATION SELF-DETERMINATION: A HISTORICAL GENEALOGY

Privacy as a legal interest has a fascinating yet controversial intellectual history. The definition of privacy put forward by Warren & Brandeis in their famous 1890 article on "the right to privacy" focused on physical invasion and the misappropriation of one's private self by the press. Alan Westin's later gave the definition of privacy as 'the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent the information about them is communicated to others'⁸, more directly anticipated the informational dimension that AI governance now demands.

The most constitutionally significant articulation of informational privacy came from the German Federal Constitutional Court in the 1983 Census Judgment (*Volkszählungsurteil*), which declared that every person possesses the fundamental right to informational self-determination, as well as the right

to decide for oneself what personal data to disclose, to whom, and for what purpose.⁹ This principle subsequently permeated European data protection philosophy, finding expression in the Council of Europe's Convention 108 (1981) and, ultimately, the General Data Protection Regulation.¹⁰

The Supreme Court initially hedged in *Govind v. State of Madhya Pradesh* (1975) and *R. Rajagopal v. State of Tamil Nadu* (1994) before decisively resolving the doctrinal ambiguity in *Puttaswamy* (2017). The nine-judge panel unanimously decided that privacy is a basic right under Articles 14, 19, and 21 of the Constitution and that one of the most important contemporary manifestations of this right is the informational dimension.

The regulatory response to this constitutional mandate has been ~~un~~ful. India enacted the Information Technology Act in 2000, with the Sensitive Personal Data or Information (SPDI) Rules appended in 2011, but these instruments were plainly inadequate for the age of big data and AI.¹¹ The Srikrishna Committee Report of 2018 recommended the comprehensive data protection framework grounded in the Puttaswamy proportionality standard, fiduciary obligation, and purpose limitation.¹² The Personal Data Protection Bill of 2019 lapsed without enactment;¹³ its successor, the DPDPA 2023, ultimately emerged as a leaner

⁸Alan Westin, *Privacy and Freedom* (Atheneum, 1967) 7.

⁹Bundeszentrale für politische Bildung / Federal Constitutional Court (Germany) — *Volkszählungsurteil* (Census Judgment), BVerfGE 65,1 (1983).

¹⁰Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation), OJ L 119/1, 4 May 2016.

¹¹Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India); Information Technology

(Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

¹²Srikrishna Committee, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* — Report of the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (Government of India, Ministry of Electronics and Information Technology, July 2018).

¹³Personal Data Protection Bill, 2019 (Lapsed). The bill was withdrawn by the government of India in August 2022 and replaced by the Digital Personal Data Protection Act, 2023.



statute with commendable digital infrastructure but significant doctrinal concessions.¹⁴

1. THE ANATOMY OF AI-DRIVEN DATA EXTRACTION ON SOCIAL MEDIA

3.1 Algorithmic Profiling and Behavioural Inference

Social media AI in today's world utilises at least four different ways of data extraction, with varying degrees of impact on privacy concerns. To begin with, "declared data" refers to information intentionally shared by people, like names, location, and preferences, which is least concerning in terms of privacy. Next, observed data refers to user behaviour that is recorded, including scrolling and other activities. Third, **inferred data** attributes derived by AI models from observed behavioural signals, including political ideology, mental health status, religious affiliation, and purchasing intent, represent the most privacy-invasive and regulatorily under-addressed category.¹⁵ Fourth, surveillance at a scale qualitatively distinct from any single platform's gathering is made possible by aggregated derived data insights produced by merging individual profiles across platforms and data brokers.

Zuboff's concept of 'behavioural surplus' captures the economic logic underlying this architecture: platforms extract more behavioural data than is necessary to improve services, with the surplus deployed to predict and shape user behaviour for third-party commercial purposes.¹⁶ Mayer-Schönberger and Cukier's foundational work on big data further demonstrated that large-scale correlative analysis can reveal

sensitive information that subjects never consciously disclosed and never would have consented to disclose.

3.2 Facial Recognition, Sentiment Analysis, and Cross-Platform Tracking

Social media companies are increasingly using biometric AI systems in addition to textual and behavioural data. Biometric identifiers that are intrinsically persistent, uniquely identifiable, and impossible to revoke upon compromise are processed by facial recognition technology, which is used for tag recommendations and authentication. *Meta's* facial recognition system, discontinued in 2021 following regulatory pressure, had processed the biometric data of hundreds of millions of users.¹⁷

In order to deduce emotional states and psychological vulnerabilities, sentiment analysis algorithms analyse linguistic and paralinguistic cues, word choice, posting frequency, emoji usage, and reaction patterns. These inferences are commercially valuable for advertisers seeking emotionally susceptible audiences and politically valuable for campaigns seeking persuadable voters.¹⁸ Pasquale's critique of the 'black box society' is particularly resonant here: the inferential logics of these systems are proprietary, opaque, and effectively insulated from public or judicial scrutiny.¹⁹

Third-party cookies, device fingerprinting, cross-site scripting beacons, and data broker middlemen enable cross-platform tracking, which makes it possible to create unified surveillance profiles that go beyond the ecosystem of any one platform. The data permanence inherent in these profiles means that the 'right to be

¹⁴Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

¹⁵Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Houghton Mifflin Harcourt, 2013) 152–154.

¹⁶Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs, 2019) 8–11

¹⁷Arjun Kharpal, 'Facebook Paid Contractors to Transcribe Users' Audio Chats' (CNBC, 13 August 2019).

¹⁸Yael Eisenstat, 'I Worked on Political Ads at Facebook.' 'Here's Why I'm Worried About the 2020 Election' (Washington Post, 4 October 2019).

¹⁹Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press, 2015) 3–6.



forgotten,' recognised in Indian constitutional jurisprudence²⁰ and codified in the GDPR's Article 17, is practically difficult to vindicate against distributed AI inference systems.²¹

1. THE INDIAN LEGAL AND REGULATORY FRAMEWORK

4.1 The Information Technology Act, 2000, and the SPDI Rules, 2011

The Information Technology Act, 2000, which is the master piece of legislation regulating the handling of electronic information in India, was primarily enacted to deal with cybercrimes and online transaction security purposes. Section 43A, added to the IT Act via the 2008 Amendment Act, provides for a duty of care and owner's liability owed by the 'body corporates' that process sensitive personal information of any individual and civil liabilities for negligent handling of data. The SPDI Rules of 2011 provide a list of sensitive personal data and prescribe a standard for the processing, use, and sharing of such data. But the current regime is riddled with serious gaps: in light of the emergence and growth of AI, it applies only to corporations; is silent on governmental institutions; does not take into consideration inferential data or algorithms; and fails to recognise the right to access and correction of personal data by individuals. However, these rules address content moderation rather than data protection, and their constitutionality with respect to traceability provisions has been challenged before multiple High Courts.²²

4.2 The Digital Personal Data Protection Act, 2023: Architecture and Critique

The DPDPA, 2023, represents the India's foremost comprehensive attempt at data protection legislation.²³ Its architecture establishes a consent-based framework for 'data fiduciaries', a Data Protection Board of India (DPBI) as the adjudicatory authority, and a set of rights for 'data principals' (individuals), including the rights to access, correction, erasure, and grievance redressal, and nomination. The Act envisages tiered compliance obligations for 'significant data fiduciaries', a category likely to capture large social media platforms, including data protection impact assessments and the appointment of data protection officers.²⁴

There are 3 categories that are discussed under doctrinal analysis, which concern AI governance on social media. **First, the consent regime.** The Act permits 'deemed consent' in broad circumstances and allows the central government to specify additional 'legitimate uses' by notification, a delegation of legislative power that lacks the precision and foreseeability required by the proportionality standard articulated in *Puttaswamy*.²⁵ "Deemed consent" is insufficient to safeguard informational self-determination in AI-driven profiling when the inference goes well beyond the declared goal of collecting.

Second, governmental exemptions. Under section 17 of the act, the central government may exempt governmental entities from virtually all of the Act's

²⁰Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, ¶ 310 per Kaul J. (recognizing the right to be forgotten as an aspect of privacy).

²¹Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation), OJ L 119/1, 4 May 2016.

²²Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India) (striking down s. 66A of the IT Act, 2000 as unconstitutional).

²³Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

²⁴DPDPA, 2023, s. 4(1) read with s. 6 (lawful processing and consent); s. 7 (legitimate uses); s. 12–13 (rights of data principal).

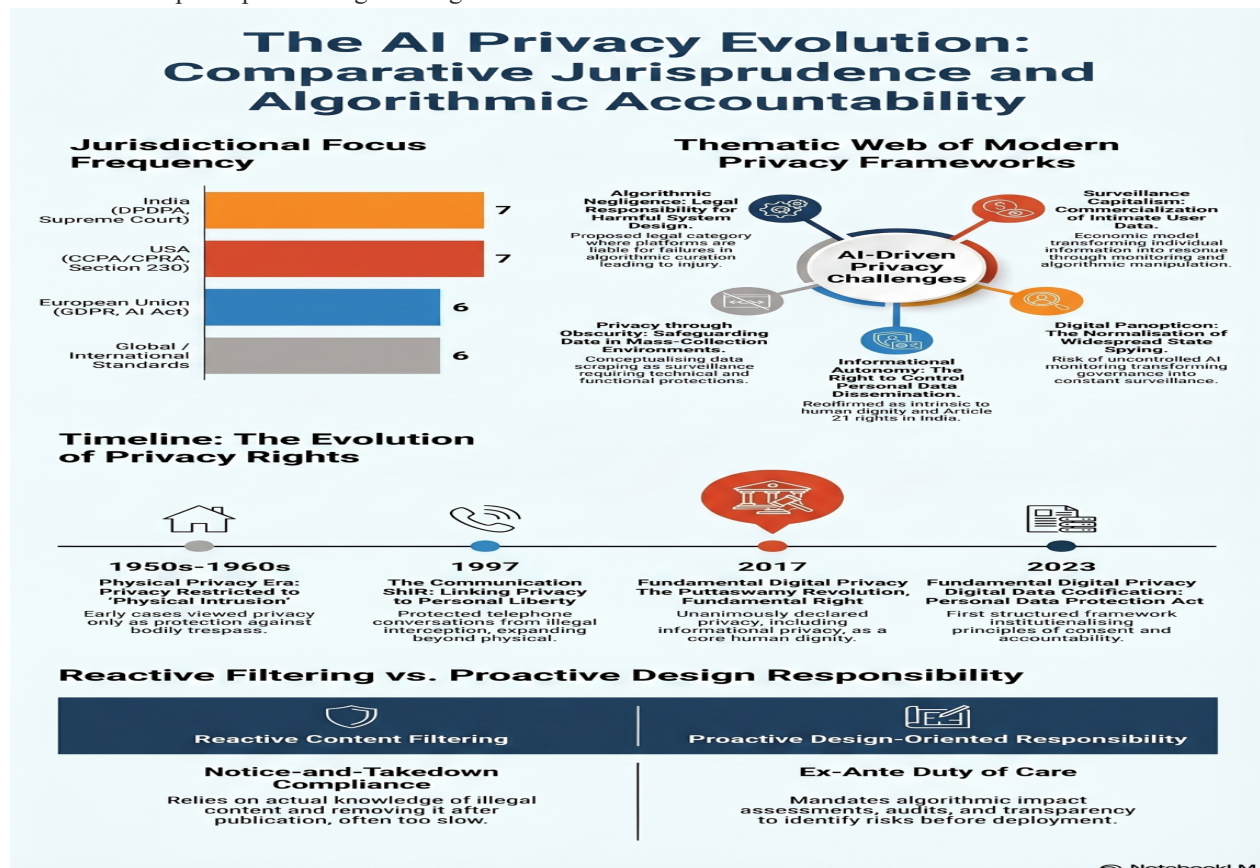
²⁵DPDPA, 2023, ss. 17–18 (exemptions for State instrumentalities and national security); cf. Puttaswamy (n 1) ¶¶ 180–185 (proportionality test).



substantive obligations on national security, public order, and sovereignty grounds. The absence of a proportionality or necessity standard for these exemptions departs materially from the Srikrishna Committee's recommendations²⁶ and from the constitutional standard set in *Puttaswamy*, where the Court held the view that any invasion of privacy must satisfy a three-part test of legality, necessity, and proportionality.²⁷

Third, algorithmic accountability. The DPDPA contains no explicit provision governing automated

decision-making, algorithmic profiling, or AI-specific risk assessment. This is a significant lacuna: the most privacy-invasive activities of social media AI systems, sentiment inference, behavioural targeting, and cross-platform tracking are simply not addressed by the Act's operational framework.²⁸ The contrast with the GDPR's Article 22, which provides a right not to be subject to solely automated decisions, and the EU AI Act's risk-based architecture for high-impact AI systems, is stark.²⁹



²⁶Srikrishna Committee, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians — Report of the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (Government of India, Ministry of Electronics and Information Technology, July 2018).

²⁷Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, ¶¶ 127, 144 per Chandrachud J.

²⁸Reuben Binns, 'Algorithmic Accountability and Public Reason' (2018) 31(4) Philosophy & Technology 543.

²⁹GDPR, art. 22; EU AI Act 2024, art. 86 (right to explanation for decisions by high-risk AI systems affecting individuals).



1. COMPARATIVE REGULATION FRAMEWORKS: GDPR AND THE EU AI

5.1 The General Data Protection Regulation, 2018

When GDPR remains the world's most influential data protection instrument, its provisions are directly relevant to AI-driven social media profiling and merit detailed doctrinal attention.³⁰ Article 5's data minimization and purpose limitation principles, which require that data be collected for specific, explicit purposes and not processed in a way incompatible with those purposes, pose the most direct regulatory challenge to social media's economic model, which depends on repurposing behavioral data for inferential advertising. As mentioned in Article 22, it confers on data subjects the right not to be subjected to a decision based solely on automated processing of data when that decision produces legal or similarly significant effects. While the article's scope is debated, Wachter, Mittelstadt, and Floridi argued that it does not create a genuine right to explanation for all automated decisions.³¹ It nonetheless establishes that the principle of AI-generated decisions might be affecting the individuals who require human oversight and a measure of explicability. This principle is further reinforced by the GDPR's recitals, which require that logic, significance, and envisaged consequences of automated processing be disclosed to data subjects.

The GDPR's extra-territorial reach, exemplified by the *Schrems II* ruling, which invalidated the EU-US Privacy Shield on grounds of inadequate protection

against US intelligence surveillance³² demonstrates that data protection law can operate as a geopolitical instrument, creating pressure on third-country regulators, including India, to align domestic frameworks with international standards.³³

5.2 The EU Artificial Intelligence Act, 2024: A Risk-Based Architecture:

The European Union Artificial Intelligence Act, which came into force in August 2024, establishes the world's first and most comprehensive regulatory framework specifically designed for AI systems.³⁴ Its risk-based architecture classifies AI systems into four categories: unacceptable risk (prohibited), high risk (heavily regulated), limited risk (transparency obligations), and minimal risk (self-regulation) and imposes obligations calibrated to these classifications.³⁵

There are three reasons why the EU AI Act is important for comparative AI governance research. First, it shows that risk-based, ex ante regulation of AI is possible from a legislative standpoint. Second, it makes "fundamental rights impact assessments" a common tool for AI governance. Third, it expresses a clear normative commitment to dignity and democratic ideals that goes beyond conventional data protection by outlawing several AI operations, especially social scoring and real-time biometric surveillance in public areas. India's DPDPA, by contrast, contains none of these AI-specific provisions, creating an asymmetry that social media

³⁰Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation), OJ L 119/1, 4 May 2016.

³¹Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7(2) International Data Privacy Law 76.

³²*Schrems II* — Data Protection Commissioner v. Facebook Ireland Limited and Maximilian

Schrems, [2020] EUECJ C-311/18 (Court of Justice of the European Union).

³³Anupam Chander and Uyen P. Le, 'Data Nationalism' (2015) 53 Emory Law Journal 677, 690.

³⁴Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (EU Artificial Intelligence Act), OJ L 2024/1689, 12 July 2024.

³⁵EU AI Act 2024, art. 5 (prohibited AI practices), art. 6–7 (high-risk AI classification), Annex III.



platforms operating across both jurisdictions may exploit through regulatory arbitrage.³⁶

6. JUDICIAL RESPONSES: PRIVACY JURISPRUDENCE AND ITS LIMITS

6.1 Puttaswamy and the Constitutional Foundation

The cornerstone of Indian privacy legislation is the ruling in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017). The constitutional foundation for data protection laws was formed by the nine-judge bench's unanimous recognition of privacy as a fundamental right under Article 21 and its clear acceptance of informational privacy as a vital aspect of that right. Justice Chandrachud's concurring opinion was particularly prescient in engaging with the digital dimension: it was observed by the leading judge that in the information age, the right to privacy encompasses the right of individuals to control personal information about themselves, to maintain a dignified existence, and to prevent the dissemination of information that violates personal autonomy.³⁷

Equally significant was the Court's adoption of a three-part proportionality test: any invasion of privacy must be (i) sanctioned by law; (ii) necessary in the service of a legitimate state aim; and (iii) proportionate, meaning the employed must be rationally connected to the aim and no more intrusive than necessary. This test provides the constitutional standard against which both the DPDPA's governmental exemptions and any future AI governance framework must be measured.³⁸

6.2 Ancillary Jurisprudence

In addition to Puttaswamy, a number of other court rulings are pertinent to privacy governance mediated by AI. In PUCL v. Union of India (1997), the Supreme Court established protections against state surveillance that, in theory, foresee the issues of AI spying and declared that the privacy of communication is a basic right guaranteed under Article 21 in relation to telephone tapping. The Court ruled in Selvi v. State of Karnataka (2010) that coercive information extraction through narco-analysis and polygraph testing violates Article 20(3)'s protection against self-incrimination. This ruling has important implications for the involuntary extraction of behavioural and biometric data by AI systems, which may be a contemporary equivalent of the coercive testimonial practices the Court denounced.

In Shreya Singhal v. Union of India (2015), the Court declared that digital communications are fully protected by basic rights, overturning Section 66A of the IT Act as an unconstitutional restriction on free expression. The judgment implicitly had recognised that chilling effects, also the phenomenon of self-censorship induced by the awareness of surveillance, can constitute a constitutional harm, a point directly relevant to the 'chilling effect' thesis of AI surveillance scholarship.³⁹

The European Court of Justice's ruling in *Google Spain v. AEPD* (2014)⁴⁰ established the 'right to be forgotten,' the right to have search results delisted where the data is inadequate, irrelevant, or no longer relevant. Kaul J.'s concurrence in *Puttaswamy* expressly acknowledged the relevance of this right to Indian constitutional law.⁴¹ Its use in AI inference

³⁶Anupam Chander and Uyen P. Le, 'Data Nationalism' (2015) 53 Emory Law Journal 677, 690.

³⁷Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, ¶¶ 127, 144 per Chandrachud J.

³⁸Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, ¶¶ 127, 144 per Chandrachud J.

³⁹Alessandro Acquisti, Laura Brandimarte and George Loewenstein, 'Privacy and Human Behavior

in the Age of Information' (2015) 347(6221) Science 509.

⁴⁰Google Spain SL v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, [2014] EUECJ C-131/12, [2014] QB 1022.

⁴¹Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, ¶ 310 per Kaul J. (recognising the right to be forgotten as an aspect of privacy).



systems, where data is constantly processed to provide new predictions rather than just stored, is still uncharted territory.

7. NORMATIVE GAPS: THE DISTANCE BETWEEN LAW AND LIVED REALITY

7.1 The Consent Paradox

Consent is the major structural keystone that works for the data protection frameworks, yet the behavioral economics and empirical studies consistently demonstrate that 'notice and consent' mechanisms as deployed by social media platforms produce only the fiction of informed choice.⁴² Authors like Acquisti, Brandimarte, and Loewenstein's foundational research demonstrated that users systematically underestimate the privacy costs of data disclosure due to cognitive biases, including present bias, the 'privacy paradox,' and bounded rationality, making 'free and informed consent' a structural impossibility in the social media context.

AI-specific aspects of the social media ecosystem exacerbate the issue: there is no discernible connection between the data collection goals revealed at the time of consent and the inferential applications to which it is subsequently put. When a user agrees to location data collecting for "service improvement," they cannot reasonably expect that this information will be used in conjunction with browsing habits, device fingerprinting, and social graph analysis to determine their political views and susceptibility to particular advertisements. The concept of 'contextual integrity,' Nissenbaum's theory that privacy is violated

when information flows across contextual norms, captures this mismatch precisely.⁴³ Neither the DPDPA nor the IT Act adequately addresses this contextual incommensurability.⁴⁴

7.2 Algorithmic Opacity and Accountability Deficits

The accountable deficit at the heart of AI governance in India is first and foremost a structural gap in the DPDPA that imposes an obligations on data fiduciaries for the purposes of data collection and processing but creates no mechanism for ongoing algorithmic accountability, no audit rights and reports, no impact assessment requirements, no explainability obligations, and no independent technical oversight of algorithmic systems.⁴⁵ In the Pasquale's description of algorithmic systems as 'black boxes' is descriptively accurate for most social media's artificial intelligence; the ranking algorithms of recommendation engines, the inferential models of sentiment analysers, and the targeting logic of behavioural advertising systems are proprietary trade secrets, shielded from regulatory scrutiny by a combination of contractual confidentiality and the absence of statutory disclosure requirements.⁴⁶

The GDPR's Article 22 and the EU AI Act's mentions about the transparency provisions and represent an alternative regulatory philosophy, which is grounded in the principle that individuals affected by consequential automated decisions have a right to a meaningful explanation of the decision-making logic.⁴⁷ Meanwhile, Wachter, Mittelstadt, and Floridi's critique that Article 22 falls to explain the

⁴²Alessandro Acquisti, Laura Brandimarte and George Loewenstein, 'Privacy and Human Behavior in the Age of Information' (2015) 347(6221) Science 509.

⁴³Woodrow Hartzog and Evan Selinger, 'Obscurity: A Better Privacy Framework than Consent' (2013) 109 Northwestern Law Review Colloquy 117.

⁴⁴DPDPA, 2023, s. 4(1) read with s. 6 (lawful processing and consent); s. 7 (legitimate uses); s. 12–13 (rights of data principal).

⁴⁵Reuben Binns, 'Algorithmic Accountability and Public Reason' (2018) 31(4) Philosophy & Technology 543.

⁴⁶Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press, 2015) 3–6.

⁴⁷GDPR, art. 22; EU AI Act 2024, art. 86 (right to explanation for decisions by high-risk AI systems affecting individuals).



genuine right to explanation⁴⁸ and underscores the difficulty of translating this principle into effective doctrine but does not negate in its normative importance. India's silence on this dimension in the DPDPA is a significant omission and depicts a huge regulatory gap.

7.3 The Surveillance-Personalisation Conflation

The deepest normative problem, perhaps, in AI governance on social media is what might be termed the surveillance-personalization conflation, meaning that the systematic presentation of surveillance as service is being blurred by the invasive tracking. As per Zuboff's analysis of surveillance capitalism demonstrates that platforms have a structural interest in obscuring the distinction between personalization, a service provided to its users, and surveillance, a service provided to advertisers, political actors, and data brokers.⁴⁹ The legal frameworks that accepts the platform framing the data processing as 'personalization' without examining the structural incentives underlying that framing are complicit in this conflation.⁵⁰

Whereas Couldry and Mejias's concept of 'data colonialism' extends this critique, as the extraction of human behavioural data by AI systems and representing a new form of colonial appropriation, in which the raw material is not land or labor but human experience itself. For users in the Global South, including the India's rapidly growing digital population, this extraction occurs in a context of acute informational asymmetry where platform of AI systems trained primarily on data from the Global

North may encode cultural and linguistic biases that systematically disadvantage Indian users, yet these users have no effective remedy under the current legal framework.⁵¹

7.4 Data Permanence and the Right to Erasure

In the principle of data permanence in AI systems creates a structural challenge for the right to erasure. Unlike traditional databases, where deletion of a record extinguishes its existence, AI inference models should learn from data during training and encode that learning in model weights that persist independently of the original data.⁵² Even if a social media platform deletes a user's declared data upon erasure request, the inferential models trained on that data and the behavioural predictions they generate continue to operate. India's DPDPA provides a right to erasure of personal data but does not address this model-persistence problem. The GDPR faces the same challenge, and the technical literature on 'machine unlearning' is still in its infancy.

8. TOWARDS A RIGHTS-CENTRED FRAMEWORK FOR AI GOVERNANCE ON SOCIAL MEDIA

8.1 Meaningful Consent and Contextual Integrity

The consent architecture of social media AI governance must be redesigned in such a way that the principle of contextual integrity is upheld and the data should flow in ways that it matches the norms of the

⁴⁸Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7(2) International Data Privacy Law 76.

⁴⁹Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs, 2019) 8–11.

⁵⁰Nick Couldry and Ulises A. Mejias, *The Costs of Connection: How Data Is Colonizing Human Life and*

Appropriating It for Capitalism (Stanford University Press, 2019) ch. 1.

⁵¹Anupam Chander and Uyen P. Le, 'Data Nationalism' (2015) 53 Emory Law Journal 677, 690.

⁵²Cynthia Dwork and Aaron Roth, 'The Algorithmic Foundations of Differential Privacy' (2014) 9(3–4) Foundations and Trends in Theoretical Computer Science 211.



context in which it was originally shared.⁵³ This calls for: (i) layered, disaggregated consent interfaces that demand separate, explicit consent for each category of inferential use; (ii) a ban on "bundled consent" that requires consent to advertising profiling to access services; (iii) a statutory presumption against secondary use of data for inferential purposes unless affirmative re-consent is obtained; and (iv) mandatory plain-language disclosure of the inferences that AI systems will draw from collected data. These requirements align with the GDPR's consent mechanism standards and would bring the DPDPA's consent framework into closer conformity with the *Puttaswamy* proportionality standard.⁵⁴

8.2 Algorithmic Explainability and Impact Assessments

Drawing on the EU AI Act's risk-based architecture, the framework proposes that all AI systems deployed by significant data fiduciaries for profiling, content recommendation, and targeted advertising be classified as 'consequential AI systems' subject to mandatory obligations including: (i) pre-deployment algorithmic impact assessments, evaluating risks to privacy, non-discrimination, and autonomy; (ii) ongoing audit rights for the Data Protection Board; (iii) a statutory right to explanation for individuals who receive content that has been targeted on the basis of inferential profiling; and (iv) mandatory disclosure of the major variables influencing recommendation or targeting decisions.⁵⁵ The DPBI should be empowered — and resourced — to conduct independent technical audits of AI systems used by significant data fiduciaries.⁵⁶

8.3 Purpose Limitation and Data Minimisation

The social media AI behavioural surplus model is structurally dependent on gathering and storing more data than is required to deliver services. This paradigm would be immediately challenged by a strong purpose limitation criteria that mandates that inferential AI systems only handle data that is absolutely necessary for the particular, declared goal. The framework proposes: (i) a statutory prohibition on the use of data collected for service improvement or for advertising profiling without separate users' consent; (ii) a mandatory data minimisation audits as part of the impact assessment process; (iii) an automatic data expiry default for categories of a sensitive inferential data; and (iv) a prohibition on the sale or licensing of inferential profiles to data brokers or third-party advertisers without data-principal consent.⁵⁷

8.4 An Independent, Technically Competent Regulatory Authority

As it is, the DPDPA's Data Protection Board lacks the technical know-how and institutional independence necessary to oversee AI systems at the scale and complexity of large social media platforms. According to the framework, the DPBI should be reorganised as a truly independent body that is not subject to executive orders. Its mandate should include AI governance, a membership of technical experts, and the authority to issue legally binding algorithmic audit findings, impose significant fines, and mandate design changes for AI systems that do not comply. The model of the UK's Information Commissioner's Office and the EU's national data

⁵³Woodrow Hartzog and Evan Selinger, 'Obscurity: A Better Privacy Framework than Consent' (2013) 109 Northwestern Law Review Colloquy 117.

⁵⁴Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, ¶¶ 127, 144 per Chandrachud J.

⁵⁵Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (EU

Artificial Intelligence Act), OJ L 2024/1689, 12 July 2024.

⁵⁶Reuben Binns, 'Algorithmic Accountability and Public Reason' (2018) 31(4) Philosophy & Technology 543.

⁵⁷Bert-Jaap Koops et al, 'A Typology of Privacy' (2017) 38(2) University of Pennsylvania Journal of International Law 483.



protection authorities are under the GDPR and provides for the useful comparative reference points.⁵⁸

8.5 International Harmonisation and Cross-Border Enforcement

Social media AI systems are inherently trans-jurisdictional, and unilateral national regulation creates the risk of regulatory arbitrage platforms structuring data flows to exploit the weakest jurisdiction in their operational footprint.⁵⁹ The framework proposes that the India actively engage in international AI governance initiatives, including OECD AI Principles, the Global Partnership on AI, and bilateral data protection adequacy negotiations with the EU to align domestic AI governance standards with international best practice. The conclusion of a data adequacy arrangement with the European Union would significantly strengthen the leverage of Indian data principals against platform AI systems by subjecting cross-border data flows to GDPR-equivalent protection.

9. CONCLUSION

AI's incorporation into social media platforms has created an incredibly sophisticated and ubiquitous data extraction ecosystem that functions well beyond the current Indian data protection legislation. Although the DPDPA, 2023, is a huge legislative improvement over the SPDI framework of the IT Act, it has substantial normative gaps concerning algorithmic responsibility, meaningful consent, governmental exemptions, and transparency duties particular to AI.

This paper's doctrinal analysis shows that these gaps are not coincidental; rather, they are the result of

intentional legislative decisions that put platform corporate interests and state operational flexibility ahead of data principals' informational self-determination.

The constitutional standard established in *Puttaswamy* that privacy invasions must be necessary, proportionate, and legally precise provides the framework within which these choices must ultimately be evaluated and, where necessary, judicially corrected.⁶⁰

The comparative analysis shows that alternative legislative architectures are available: the EU AI Act's risk-based, explainability-centred approach and the GDPR's purpose limitation and automated decision rights offer doctrinal models that can be modified without complete transplantation to India's constitutional and developmental context. Based on the *Puttaswamy* proportionality norm, responsive to the unique privacy risks of AI-driven social media, and in line with the growing global agreement on responsible AI governance, the five-principle framework put forth in Section VIII offers a rights-centered path forward.

The necessity of this governance recalibration only increases as social media AI systems become more potent, progressing from profiling and targeting to prediction, manipulation, and the creation of synthetic personhood. Without the social media ecosystem risks normalizing the pervasive surveillance under the guise of personalization, the constitutional right to privacy is transformed from a fundamental freedom into a formal declaration without practical content.⁶¹

⁵⁸Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation), OJ L 119/1, 4 May 2016.

⁵⁹Anupam Chander and Uyen P. Le, 'Data Nationalism' (2015) 53 Emory Law Journal 677, 690.

⁶¹Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs, 2019) 8–11.



BIBLIOGRAPHY

A. Primary Sources

Legislation and Regulations

Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council, OJ L 119/1, 4 May 2016 (GDPR).

Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, 2009 (India).

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (India).

Personal Data Protection Bill, 2019 (Lapsed) (India).

Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (EU Artificial Intelligence Act), OJ L 2024/1689, 12 July 2024.

UK Data Protection Act, 2018, c.10 (United Kingdom).

Cases

Bundeszentrale für politische Bildung / Federal Constitutional Court (Germany) — Volkszählungsurteil (Census Judgment), BVerfGE 65,1 (1983).

Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems (Schrems II), [2020] EUECJ C-311/18 (CJEU).

Google Spain SL v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, [2014] EUECJ C-131/12.

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

PUCL v. Union of India, (1997) 1 SCC 301 (India).
Selvi v. State of Karnataka, (2010) 7 SCC 263 (India).
Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).

B. Secondary Sources

Articles and Book Chapters

Acquisti, Alessandro, Laura Brandimarte and George Loewenstein, 'Privacy and Human Behavior in the Age of Information' (2015) 347(6221) Science 509.

Barocas, Solon and Moritz Hardt, 'Fairness in Machine Learning' (NeurIPS Tutorial, 2017) <<https://fairmlbook.org>>.

Binns, Reuben, 'Algorithmic Accountability and Public Reason' (2018) 31(4) Philosophy & Technology 443.

Chander, Arpanam and Uyen P. Le, 'Data Nationalism' (2015) 53 Emory Law Journal 677.

Dwork, Cynthia and Aaron Roth, 'The Algorithmic Foundations of Differential Privacy' (2014) 9(3-4) Foundations and Trends in Theoretical Computer Science 211.

Hartzog, Woodrow and Evan Selinger, 'Obscurity: A Better Privacy Framework than Consent' (2013) 109 Northwestern Law Review Colloquy 117.

Koops, Bert-Jaap et al, 'A Typology of Privacy' (2017) 38(2) University of Pennsylvania Journal of International Law 483.

Selbst, Andrew D. and Solon Barocas, 'The Intuitive Appeal of Explainable Machines' (2018) 87(3) Fordham Law Review 1085.

Wachter, Sandra, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7(2) International Data Privacy Law 76.

Citron, D. K., & Pasquale, F. (2014). The scored society: Due process for automated predictions. *Washington Law Review*, 89(1), 1-33.

De Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer*



Law & Security Review, 32(2), 179–194.
<https://doi.org/10.1016/j.clsr.2016.02.006>

Jones, K., Zahrah, F., & Nurse, J. R. C. (2024). *Embedding privacy in computational social science and artificial intelligence research*. arXiv.
<https://arxiv.org/abs/2404.11515>

Kedare, A., & Jeswani, D. (2024). Impact of social media on individual's right to privacy. *Journal of Constitutional Law and Jurisprudence*.

Lewis, D., & Moorkens, J. (2020). A rights-based approach to trustworthy AI in social media. *Social Media + Society*, 6(3).
<https://doi.org/10.1177/2056305120954672>

Malgieri, G., & Comandé, G. (2017). Why a right to legibility of automated decision-making exists in the General Data Protection Regulation. *International Data Privacy Law*, 7(4), 243–265.
<https://doi.org/10.1093/idpl/ix019>

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, 79(1), 119–157.

Ploug, T. (2023). The right not to be subjected to AI profiling based on publicly available data—Privacy and the exceptionalism of AI profiling. *Philosophy & Technology*, 36(1), 1–22.
<https://doi.org/10.1007/s13347-023-00616-9>

Tandon, U., & Gupta, N. K. (2025). Informational privacy in the age of artificial intelligence: A critical analysis of India's DPDP Act, 2023. *Legal Issues in the Digital Age*, 6(2), 87–117.
<https://doi.org/10.17323/2713-2749.2025.2.87.117>

Verma, K. (2024). Digital deception: The impact of deepfakes on privacy rights. *Lex Scientia Law Review*, 8(2). <https://doi.org/10.15294/lslr.v8i2.13749>

Wachter, S., & Mittelstadt, B. (2019). A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI. *Columbia Business Law Review*, 2019(2), 494–620.
<https://doi.org/10.7916/cblr.v2019i2.3424>

Zeide, E. (2025). Expanding the paradigm: Generative artificial intelligence and U.S. privacy norms. *Cambridge Forum on AI: Law and Governance*.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

Books

Couldry, Nick and Ulises A. Mejias, *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism* (Stanford University Press, 2019).

Mayer-Schönberger, Viktor and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Houghton Mifflin Harcourt, 2013).

Pasquale, Frank, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press, 2015).

Westin, Alan, *Privacy and Freedom* (Atheneum, 1967).

Zuboff, Shoshana, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs, 2019).

Reports and Other Sources

European Commission, 'Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)' COM(2017) 10 final, 10 January 2017.

Law Commission of India, Report No. 288: 'Digital Personal Data Protection Bill, 2022 — A Critical Analysis' (2023).

Srikrishna Committee, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Ministry of Electronics and Information Technology, Government of India, July 2018).

OECD, 'Recommendation of the Council on Artificial Intelligence' OECD/LEGAL/0449 (22 May 2019).