



INDIAN JOURNAL OF LEGAL AFFAIRS AND RESEARCH

VOLUME 3 ISSUE 1

Peer-reviewed, open-access, refereed journal

IJLAR

+91 70421 48991
editor@ijlar.com
www.ijlar.com

DISCLAIMER

The views and opinions expressed in the articles published in the Indian Journal of Legal Affairs and Research are those of the respective authors and do not necessarily reflect the official policy or position of the IJLAR, its editorial board, or its affiliated institutions. The IJLAR assumes no responsibility for any errors or omissions in the content of the journal. The information provided in this journal is for general informational purposes only and should not be construed as legal advice. Readers are encouraged to seek professional legal counsel for specific legal issues. The IJLAR and its affiliates shall not be liable for any loss or damage arising from the use of the information contained in this journal.

IJLAR

Introduction

Welcome to the Indian Journal of Legal Affairs and Research (IJLAR), a distinguished platform dedicated to the dissemination of comprehensive legal scholarship and academic research. Our mission is to foster an environment where legal professionals, academics, and students can collaborate and contribute to the evolving discourse in the field of law. We strive to publish high-quality, peer-reviewed articles that provide insightful analysis, innovative perspectives, and practical solutions to contemporary legal challenges. The IJLAR is committed to advancing legal knowledge and practice by bridging the gap between theory and practice.

IJLAR

Preface

The Indian Journal of Legal Affairs and Research is a testament to our unwavering commitment to excellence in legal scholarship. This volume presents a curated selection of articles that reflect the diverse and dynamic nature of legal studies today. Our contributors, ranging from esteemed legal scholars to emerging academics, bring forward a rich tapestry of insights that address critical legal issues and offer novel contributions to the field. We are grateful to our editorial board, reviewers, and authors for their dedication and hard work, which have made this publication possible. It is our hope that this journal will serve as a valuable resource for researchers, practitioners, and policymakers, and will inspire further inquiry and debate within the legal community.

IJLAR

Description

The Indian Journal of Legal Affairs and Research is an academic journal that publishes peer-reviewed articles on a wide range of legal topics. Each issue is designed to provide a platform for legal scholars, practitioners, and students to share their research findings, theoretical explorations, and practical insights. Our journal covers various branches of law, including but not limited to constitutional law, international law, criminal law, commercial law, human rights, and environmental law. We are dedicated to ensuring that the articles published in our journal adhere to the highest standards of academic rigor and contribute meaningfully to the understanding and development of legal theories and practices.

IJLAR

DIGITIZED GLOBAL MOVEMENT WITH ADHERENCE TO HUMAN RIGHTS AND FUNDAMENTAL RIGHTS: OBSERVING CURRENT DATA AND CHALLENGES.

AUTHORED BY - MS. SUPRIYA¹ & MR. DEEPAK KUMAR PANDEY²

In the current digital era, the traditional difference between fundamental rights and human rights is increasingly hampered as both sets of rights encounter a data-driven environment arising out of the internet, AI governance and cross-border surveillance. As enunciated in the Universal Declaration of Human Rights (UDHR) and other recognised treaties, human rights remain fully enforceable in digital spaces. Moreover, the UDHR also includes the right to privacy, equality, association or disassociation³. Thus, these rights are no longer constrained to physical platforms and are also extending to virtual platforms where states as well as persons jointly frame conditions for their convenience and necessary obligations.

At a fundamental level, considering the domestic sphere, fundamental rights enshrined in our Constitution, Part III serve as the basic legal shield against the interference of the state. Nonetheless, their scope must also be reiterated in view of geographical tracking, automated content moderation, face recognition technologies and uncontrolled surveillance⁴. Modern legal jurisprudence exponentially considers privacy and digital autonomy as core components of the right to life and personal liberty, subsequently compelling the state within digital parameters to satisfy tests of legality, as well as necessity. As the global movement of digital technologies increases, it further complicates the data flow across borders; however, the challenge is that the legal protection extends territorially⁵. Applications based on multinational platforms, cloud space and AI operate beyond the reach of any single national court, yet they declare awards that notably affect freedom of expression, political and economic participation. Considering this notion, digital

¹ PhD Student, Chanakya National Law University, Patna

² AOR-B/D 0783 Reg. No. 17529/2022

³ Indian institute of Legal Studies, Darjeeling, University of North Bengal.

⁴ Universal Declaration of Human Rights Art 1, U.N. Doc. (1948).

⁵ Jane Doe; *Digital Human Rights: Fundamental Freedom in the Digital Age* 45 (2024).

rights therefore emerge as a mechanism for reinforcing existing human rights protections, including concerns relating to data privacy, algorithmic bias, and equity-based digital governance within existing international and constitutional standards.

The most significant challenge within digital governance is therefore the implementation of effective state regulation, the establishment of institutional accountability and judicial interpretation in conformity with the existing international human rights framework so that human dignity, political participation and fundamental freedoms are effectively safeguarded in an increasingly interconnected and technologically driven world.

Key Words: Human Rights, Fundamental Rights, Digital Rights, Privacy, and Data Protection.

1. Introduction

The evolution of the digital era has essentially transformed the structure of governance, power, and institutions. Human rights and fundamental rights had once a clear distinction between them with respect to their scope and enforceability. This distinction has now begun to devolve due to AI, cross-border surveillance, and most potentially because of data-driven technologies. In physical boundaries, the protections granted by the constitutional guarantees and other substantive norms relating to human rights could easily be traced, identifying the area, predators, and agency/institution. In the digital space, the same rights and protections are granted; however, they are also constrained and violated by borderless infrastructures supported by AI. This situation challenges the lawful assumptions of sovereignty, jurisdiction, and enforceability⁶.

The challenge is prominently visible in the way of privacy and data protection, which were once marginal concerns in human rights and constitutional discourse as the core element of human dignity and personal liberty. Surveys from the Supreme Court of India reveal a data-based trajectory that privacy is no longer understood as secrecy or the right to isolate but only as the precondition for meaningful self-determination and autonomy and participation in a data-intensified environment. Subsequently, technologies such as facial recognition, automated

⁶ Constitution of India pt. III, arts. 12-35 (1950).

moderation of content, GPS (Global Positioning System), and algorithmic result-generating systems have spread their scope beyond permissible control and surveillance without any adequate legal safeguards or effective remedies⁷.

Henceforth, the idea of digital rights has emerged as a bridge between existing human rights and constitutional frameworks. The idea of digital rights seeks to translate already existing human rights standards into acknowledging privacy, equality, freedom of expression, and non-discrimination into the specific conditions of digital platforms and AI-based systems. In India and other constitutional democracies, this translation project raises immediate questions about the outreach of fundamental rights enumerated in Part III of the Constitution, the scope of state action on any digital platforms, and the efficacy of current governance to protect human dignity and political rights on any global platform.

This paper comprehends that the conventional difference between human rights and fundamental rights is highly pragmatic and functional at the same time. In a digital space, both sets of rights converge on the same ground of privacy, data protection, freedom of expression, and transparency in algorithmic moderation. The emerging elements of digital rights do not displace fundamental rights or human rights frameworks; rather, they encapsulate these rights within the context of digital technologies, institutional characteristics, and cross-border data flows. This paper further proceeds with four chapters ahead. Lastly, the paper will include a conclusion that presents a framework incorporating both protection and a rights-based approach to digital governance.

2. Understanding Human Rights and Fundamental Rights in the Digital Age

2.1 Human Rights in the Digitized Space: Scope and Limits.

The Universal Declaration of Human Rights (UDHR), adopted in 1948, provides the fundamental lawful standards for modern human rights contemplation. While the UDHR does not expressly mention the internet or other digital technologies, its fundamental principles are studied by both national and international bodies to apply them in both physical and digital contexts. This

⁷ *Justice Puttaswamy V. Union of India* (2017) 10 SCC

interpretation is based on the principle that human rights are dynamic and are meant to be referred to in the context of social, technological, and political conditions⁸.

These provisions, later enunciated in the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR), have been repeatedly invoked by the various United Nations (UN) bodies to affirm that the rights of an individual on a material (physical/offline) basis should also be enforced on a digitalized basis (online). Specifically, the unlawful or arbitrary interference with privacy and random and non-consented data collection, including mass surveillance, violates Article 17 of the ICCPR.

Unfortunately, and ironically, this universality is also subject to practical constraints. Human rights are enforced through institutional mechanisms such as treaties, lawful procedures, and regional courts. These institutions are scarce of jurisdictional outreach and have the same powers as those of a domestic court. Moreover, the institutional characters highly responsible for digital-rights violations are multinational technology-based companies, AI-driven platforms, and cloud-based applications. These above-mentioned platforms are pertinently beyond the effective control of any single state, and this unanimously creates the constraint for state and centre authorities holding power to strengthen and protect human rights.⁹

2.2 Fundamental Rights in Indian Constitutional Orders

If laws relating to human rights provide the legal baseline, fundamental rights transform these principles into enforceability. Part III of the Constitution of India enunciates the civil and political rights protections, including the right to equality (Article 14), the right against discrimination (Articles 15 and 16), the right to freedom of speech and expression (Article 19(1)(a)), and the right to life and personal liberty (Article 21). These articles are interpreted in the context of the physical environment, state-owned authorities, and digital realms.

In the digital age, the Justice K.S. Puttaswamy (Retd). The judgement in the case of Justice K.S. Puttaswamy (Retd) v. Union of India (2018) was a significant watershed moment in the Indian Constitution. The nine-judge bench unanimously declared that the 'right to privacy is an intrinsic

⁸ AC Dhabu, *Legal Implications of Artificial Intelligence in Cross Border Transactions*, Lund Univ. Student Paper (2024), <https://lup.lub.lu.se/student-papers/record/9154823/file/9154824.pdf>.

⁹ Office of the High Commissioner for Human Rights, *Digital Border Governance: A Human Rights-Based Approach* 1-2 (2023), <https://www.ohchr.org/sites/default/files/2023-09/Digital-Border-Governance-A-Human-Rights-Based-Approach.pdf>.

part of the right to life and personal liberty under Article 21' and that true privacy guarantees an individual their right to dignity, freedom of expression, and autonomy¹⁰. This judgement did substantially more than simply *recognize* privacy; it re-established the constitutional framework and scrutiny of digital governance within well-established tests of necessity, legality, proportionality, and lawful objectives¹¹.

Subsequently, other judgements have reiterated the idea that privacy and data protection are inseparable from personal liberty in the digital era. For example, the AADHAR system has highlighted that the mandatory linkage of biometric and demographic data with banking and welfare services can transform welfare-enhancing technologies into a surveillance infrastructure by default. This principle shall prevail unless it is strictly regulated. The Supreme Court's ruling in Justice K.S. Puttaswamy (Retd.) v. Union of India, along with related cases concerning AADHAR, highlights the issue of full-fledged data collection that employs a blanket approach without any express lawful objective or sufficient safeguards, thereby violating the constitutional core of privacy and dignity¹².

Thus, at the domestic level, fundamental rights are being reinterpreted and acknowledged to support the data protection frameworks of digital governance. Thus, privacy here is treated as the fundamental principle for assessing the legitimacy of state or private consumption of digital technologies, rather than as a non-primary or secondary right¹³.

2.3 Functional Complexities and Overlapping Practice.

In practice, the distinction between human rights and fundamental rights is dominantly functional. The same practice and technologies can be challenged under both universal rights and constitutionally recognized rights, often through parallel or overlapping legal rulings.

For instance, a mandatory biometric authentication under Aadhar in India has got the civil bodies and academics invoking international human rights standards on privacy, non-discrimination, and participation to argue that random and disproportionate collection of data violates the universal

¹⁰ G.A. Res. 48/141, at 2–3, U.N. Doc. A/RES/48/141 (Dec. 20, 1993).

¹¹ International Commission of Jurists, *Digital Technologies and Human Rights: Legal Framework* 3-4 (2022) , <https://www.icj.org/wp-content/uploads/2022/05/Digital-Technologies-and-Human-Rights-Briefing-Paper-FINAL-VERSION-May-2022.pdf>.

¹² Human Rights Council Res. 26/13, Para 1, U.N. Doc.A/HRC/RES/26/13 (June 26, 2014).

¹³ Universal Declaration of Human Rights, G.A. Res. 217A (III) U.N. GAOR, 3d Session, 183d plen. mtg., at 71, U.N. Doc. A/RES/ 217(III)(Dec. 10, 1948).

right to privacy and dignity. But on the other hand, domestic litigation has been found to have relied on Articles 14, 19, and 21 of the Constitution to challenge the same practices before the Indian Supreme Court, validly putting forth the right to equality, freedom of expression, and right to life and personal liberty.

This particular convergence is not new or different to India. In other jurisdictions, courts and human rights mechanisms have similarly treated digital privacy and data protection concerns as matters of both constitutional and international law significance. The European Court of Human Rights, in cases such as *Lloyd v. United Kingdom* (2018) has acknowledged the necessity in a democratic society and proportionality tests in data collection and surveillance practices, efficiently reiterating the European Convention on Human Rights while also affecting domestic-level constitutional rights discourse¹⁴.

The functional overlapping of human rights and fundamental rights laws should be read in parallel, rather than in isolation. Human rights instruments provide the normative baseline and interpretative framework for how privacy, equality, and non-discrimination should be practiced. Fundamental rights jurisprudence, in contrast, offers procedural and remedial mechanisms that make these norms enforceable before the domestic courts. In digital contexts, state and non-state actors collectively shape rights and powers¹⁵.

Enforcing infrastructure, this dual approach is vital for both doctrinal coherence and non-doctrinal efficacy. Moreover, the re-convergence of human and fundamental rights in this current digital era challenges the traditional assumption that constitutionalism is inherently territorial. While constitutional courts remain restricted due to the geographical limits of their jurisdictions, the technologies they mainly regulate are probably transnational¹⁶. The digital platforms, AI-driven applications, and cloud infrastructure invite a more cosmopolitan, inclusive reading of constitutional principles, where, for example, the Supreme Court of India may outline the international human rights standards to be imbibed in its interpretation of Articles 14, 19, and 21, even when the primary obligations of the states are owed to its citizens in prerogative.

¹⁴ Zachary Jin, *International Legal Regulation of Cross-Border Data Flows in Digital Trade*, 143941 SciTePress 619-28(2025)

¹⁵ Marietta Auer, *Autonomy and the Digital Person*, Max Planck Law Perspectives (2024), <https://law.mpg.de/perspectives/autonomy-and-the-digital-person/>.

¹⁶ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1

3. The Recalibration of Privacy and Liberty

3.1 Expansion of Surveillance with New Technologies.

The rise in location tracking tools, facial recognition, predictive algorithms, and other AI-driven tools has dramatically altered the structure of state power. These technologies enable continuous and unacknowledged surveillance, raising serious concerns about the proportionality test under human rights and constitutional law¹⁷.

Location or geographical tracking relies on the location of data aggregation from mobile devices, GPS systems, and network-based identifiers. When coupled with other systems such as financial transactions, social networking activities or voice-call recordings, the same geographical data can construct an individual's preferences, beliefs, and associations with drastic precision. Likewise, similar concerns arise with facial recognition apps, which can be deployed in public areas, airports, social media platforms, or privatized retail areas, as they acquire access without explicit consent or transparency.¹⁸

Automated content moderation, although it raises different issues, is still relatable. Different social media platforms and intermediary services use them to filter posts, videos, and comments. On one hand, the goal is to moderate hate speech or misinformation or prohibit the incitement of violence through these platforms, which is legitimate. On the other hand, the use of algorithms to blacklist or suspend accounts or demonetize content can significantly impact freedom of expression and political participation. In India, the tension between the liability of intermediaries, platform governance rules, and constitutional rights to speech and expression is threatened as courts and other legal bodies (both de facto and de jure) struggle to maintain a balance between public order and digital expression rights¹⁹.

The uninformed surveillance does not only extend to the state or central authorities. Private corporations that operate on digitized technology platforms and AI-driven commercial firms often collect, synthesize, and monetize personal data as a fundamental part of their business models. This situation disturbs the differentiating criteria for separating state-mandated surveillance and surveillance involving commercial purposes. Government agencies themselves rely heavily on

¹⁷ Lloyd (Respondent) v Google LLC (Appellant), UKSC 50, 2 ALL ER 1090.

¹⁸ Thomas Giegerich, *Human Rights and Constitutional Law: Patterns of Mutual Validation*, in *The Impact of Human Rights Law on General International Law* 117-34 (Prof. Menno T. Kamminga ed., 2015).

¹⁹ Felix M. Simon et al., *A Unifying Framework to Understand Digital Autonomy*, OSF Preprints (Feb. 25, 2026), <https://osf.io/bufmv>.

data collected by private corporations for public security and economic governance policies. The result is evidently a hybrid surveillance approach, where the boundaries of the state and private corporations are increasingly difficult to differentiate²⁰.

3.2 Right to Privacy, Data Protection, and Procure Digital Autonomy

The landmark Puttaswamy Judgement has an elementary role in re-establishing privacy not simply as a shield against state interference but also as the foundation of digital autonomy and consented access to one's personal data. This meaningful shift has serious implications for how privacy and data protection are understood in the digital era²¹. Consented access to data implies a defined control over why an individual's data is collected and for what purposes it is used, particularly in cases where an applied algorithm affects their rights and opportunities. This reinterpretation has been reiterated and combined through judicial principles and legislative undertakings. A vital piece of legislation in this context is the Digital Personal Data Protection (DPDP) Act, 2023. This act seeks to bring the concept of privacy into operation and the principles of data protection within the domestic norms, practically touching on both Indian constitutional principles and international human rights standards.²² The statute is a vital step towards establishing a formal structure for digital rights protection in Indian law. However, critics have raised concerns about the act's exemption for data requirements and processes related to national security.

Beyond basic data protection, the concept of digital autonomy has erupted as a fundamental component of both human and fundamental rights. For instance, there is an undue restriction on transparency and the right to contest automated government decisions made in collaboration with online platforms that use opaque algorithms to assign credit scores or restrict access to welfare services without reasonable explanations²³.

In practice, the erosion of digital autonomy has perpetuated in several ways as following:

1. The dangerous practice of content moderation that disproportionately restricts the voices

²⁰ Ved P. Nanda, *Constitutional Law of India* 180-90 (4th edition. Eastern Book Co. 2020).

²¹ *Device-Based Geolocation: Understanding Location Tracking*, IPinfo (Feb.5, 2025), <https://ipinfo.io/blog/device-based-geolocation>.

²² Chintan Chandrachud & CLPR, *Freedom of Speech in the Digital Age: A Doctrinal Analysis of Four Recent Supreme Court Cases on Article 19(1)(a)*, Centre for Law and Policy Research, <https://clpr.org.in/blog/a-little-over-the-top-examining-indias-new-laws-for-online-speech-part-i/>.

²³ David Gray & Stephen E. Henderson, *Big Data Surveillance: The Convergence of Big Data and Law Enforcement*, in *The Cambridge Handbook of Surveillance Law* 171, 171-97 (2017).

of dissenters, minorities, or activists, even when their speech does not meet the threshold for lawful restriction.

2. Forced enrolments under biometric and digital-ID systems without adequate safeguards or alternatives.
3. Automated systems disproportionately disadvantage marginalized communities based on gender, race, caste, or socioeconomic status.

In each of the above scenarios, the exercise of privacy and autonomy remains meaningless unless there's robust mechanisms for accountability, transparency, as redress. Human rights and fundamental rights, thus, need to be interpreted and executed to encompass not only the protection of data but also the governance of algorithms.

4. Conclusion

In this data-driven, interconnected world of the 21st century, the traditional separation between human rights and fundamental rights can no longer be sustained in a strict binary approach. Both the sets of rights are constitutional, universal, and based on entitlements from treaties. In the digital space, privacy, data protection, equality, freedom of expression, and the right against discrimination converge, leading to simultaneous compromises. The movement for digital rights does not replace these frameworks but rather operationalizes them by providing a simultaneous normative structure through which the impact of AI, surveillance, and algorithmic governance on human dignity and democratic individual participation can be evaluated.

At the constitutional level, especially in the landmark case *K.S. Puttaswamy (Retd) v. Union of India*, the judgement has reiterated privacy and data protection as core components of Article 21 (Right to life and personal liberty) while also reinforcing equality and non-discrimination under Article 14 and Article 15. This shift compels the state to address and adhere to the rigor's tests of legality, necessity, proportionality, and legitimate aim, even within the highly opaque AI-heavy digital infrastructure. Similarly, at the global level, the Office of the United Nations High Commissioner for Human Rights (OHCHR) has declared that the rights protected offline must also be protected online, thus extending the concept of human rights to cross-border data flows and digital platforms.

The territorial limits of legally enforceable rights often escape the effective jurisdiction of any single domestic or national court, especially amidst the significant challenges posed by the boundary-less nature of digital platforms and cloud-based infrastructures. Meaningful protection requires a multi-layered structure with robust regulations that incorporate fundamental principles such as human rights and constitutional values, along with versatile judicial interpretations that apply proportionality, dignity, and equality tests to digital environments, while also addressing the roles of private data protection authorities and algorithm-based firms.

For India and other democracies, the task ahead is to balance the universal aspirations of human rights law with fundamental rights while imbibing the discourse of digital rights. Only with an integrated system and a rights-based approach can the concept of human dignity be stabilized and safeguarded, which involves political participation and fundamental freedoms in an era defined by AI, cross-border surveillance and data distribution. Furthermore, legislative development in the areas of data protection, digital governance, and algorithmic moderation must be accompanied by public awareness initiatives and improved institutional engagement to ensure that people can exercise their digital rights as part of civic engagement activities.

References

1. A.C. Dhabu, *Legal Implications of Artificial Intelligence in Cross Border Transactions*, Lund University Student Paper (2024), available at: <https://lup.lub.lu.se/student-papers/record/9154823/file/9154824.pdf>.
2. Chintan Chandrachud & Centre for Law and Policy Research, *Freedom of Speech in the Digital Age: A Doctrinal Analysis of Four Recent Supreme Court Cases on Article 19(1)(a)*, available at: <https://clpr.org.in/blog/a-little-over-the-top-examining-indias-new-laws-for-online-speech-part-i/>.
3. Constitution of India, pt. III, arts. 12–35.
4. David Gray & Stephen E. Henderson, “Big Data Surveillance: The Convergence of Big Data and Law Enforcement” in *The Cambridge Handbook of Surveillance Law* 171–197 (2017).
5. Device-Based Geolocation: Understanding Location Tracking, IPinfo (Feb. 5, 2025), available at: <https://ipinfo.io/blog/device-based-geolocation>.

6. Felix M. Simon et al., *A Unifying Framework to Understand Digital Autonomy*, OSF Preprints (Feb. 25, 2026), available at: <https://osf.io/bufmv>.
7. G.A. Res. 48/141, U.N. Doc. A/RES/48/141 (Dec. 20, 1993).
8. Human Rights Council Res. 26/13, U.N. Doc. A/HRC/RES/26/13 (June 26, 2014).
9. International Commission of Jurists, *Digital Technologies and Human Rights: Legal Framework* (2022), available at: <https://www.icj.org/wp-content/uploads/2022/05/Digital-Technologies-and-Human-Rights-Briefing-Paper-FINAL-VERSION-May-2022.pdf>.
10. Indian Institute of Legal Studies, Darjeeling, University of North Bengal.
11. Jane Doe, *Digital Human Rights: Fundamental Freedom in the Digital Age* 45 (2024).
12. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
13. Lloyd v. Google LLC, [2021] UKSC 50, 2 All ER 1090.
14. Marietta Auer, *Autonomy and the Digital Person*, Max Planck Law Perspectives (2024), available at: <https://law.mpg.de/perspectives/autonomy-and-the-digital-person/>.
15. Office of the High Commissioner for Human Rights, *Digital Border Governance: A Human Rights-Based Approach* 1–2 (2023), available at: <https://www.ohchr.org/sites/default/files/2023-09/Digital-Border-Governance-A-Human-Rights-Based-Approach.pdf>.
16. Thomas Giegerich, “Human Rights and Constitutional Law: Patterns of Mutual Validation” in *The Impact of Human Rights Law on General International Law* 117–134 (Prof. Menno T. Kamminga ed., 2015).
17. Universal Declaration of Human Rights, G.A. Res. 217A (III), U.N. Doc. A/RES/217(III) (Dec. 10, 1948).
18. Ved P. Nanda, *Constitutional Law of India* 180–190 (4th edn., Eastern Book Company 2020).
19. Zachary Jin, “International Legal Regulation of Cross-Border Data Flows in Digital Trade” 143941 SciTePress 619–628 (2025).