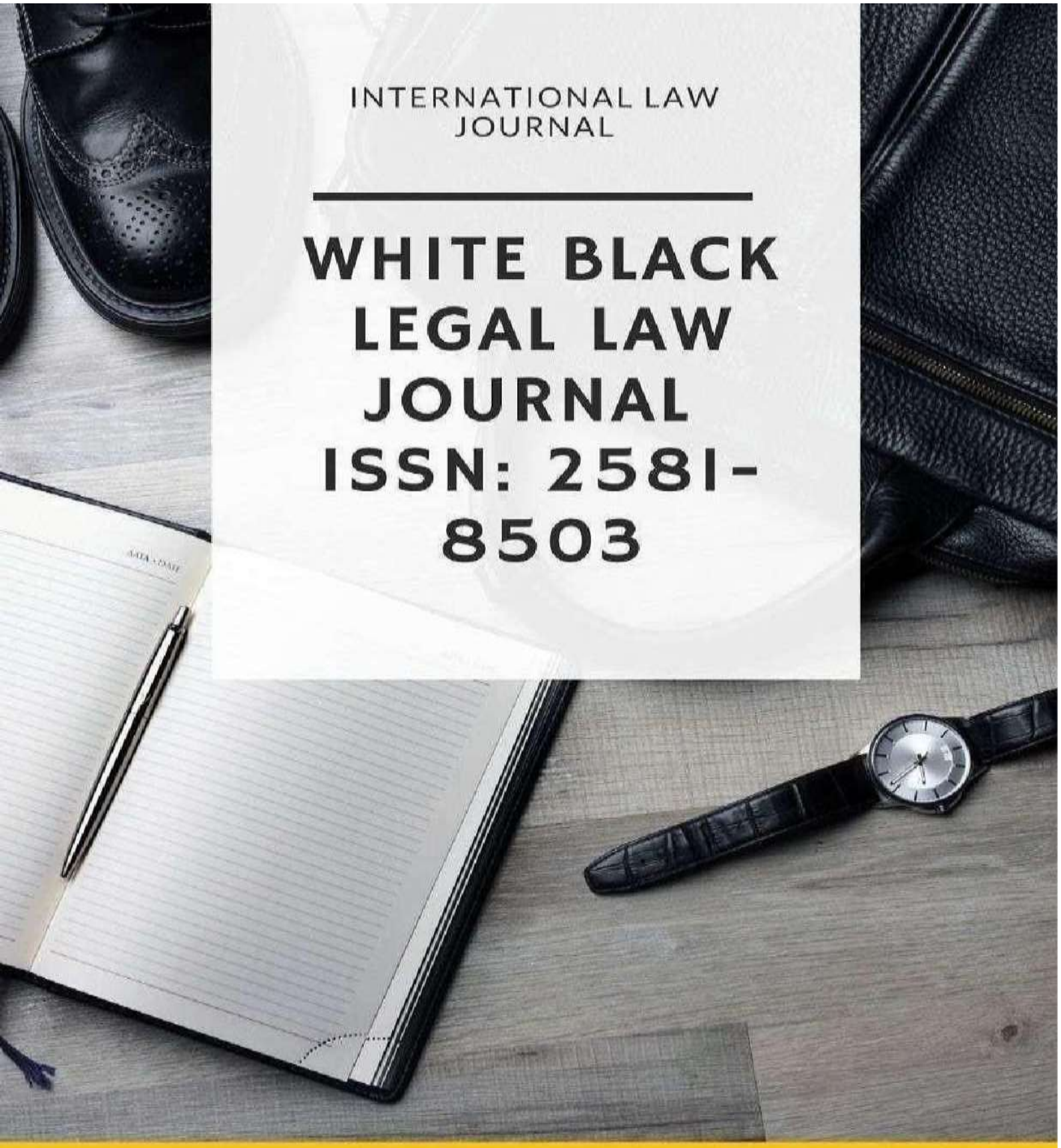

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 1 | March 2025 ISSN: 2581-8503

BEYOND CONSENT: ALTERNATIVE LEGAL AND ETHICAL FRAMEWORKS FOR USER AGREEMENTS IN THE DIGITAL AGE

AUTHORED BY - DHRUVA SHREE V
Student, School of Law, CHRIST (Deemed to be University)

Abstract

The consent-based model of digital agreements has long been regarded as the cornerstone of data protection frameworks worldwide. However, in the contemporary digital economy, consent is increasingly recognized as a legal fiction, failing to provide individuals with meaningful control over their personal data. This paper critically examines the limitations of the consent model, particularly in the Indian context, where regulatory gaps in the Digital Personal Data Protection Act, 2023 (DPDP Act) leave users vulnerable to corporate data exploitation and state surveillance. It argues that India must transition toward an accountability-based model, where corporations bear the burden of proving data fairness and necessity, rather than relying on user consent as a mere formality.

The study explores emerging legal doctrines, including data fiduciary obligations and Digital Habeas Corpus, as mechanisms to empower users and establish stronger corporate accountability. It situates India's evolving data governance framework within a comparative constitutional law perspective, drawing insights from Germany, the European Union, South Korea, and the United States.

Additionally, empirical case studies such as Aadhaar data leaks, WhatsApp's privacy controversies, and Paytm's data-sharing practices demonstrate the failures of existing consent frameworks in protecting user rights.

Beyond regulatory reforms, this paper examines technological and market-based solutions, including user-owned data markets and decentralized identity systems, as potential alternatives to traditional data governance models. It further advocates for India's proactive engagement in G20 digital governance discussions and OECD privacy guidelines, ensuring that its data

protection policies align with global best practices while safeguarding national interests.

Ultimately, this paper contends that a legal and policy shift toward fairness, transparency, and accountability is imperative for protecting user autonomy in digital agreements. By replacing the flawed consent-based approach with a rights-oriented, accountability-driven regulatory model, India can achieve a balance between privacy protection and technological innovation, fostering a more equitable and secure digital ecosystem.

Keywords

Digital consent, accountability-based model, data fiduciary obligations, Digital Habeas Corpus, data privacy, Digital Personal Data Protection Act (DPDP Act), algorithmic governance, dark patterns, comparative constitutional law, private governance, AI bias audits, user autonomy, data rights, decentralized identity, global data governance.

Introduction

The principle of consent serves as the foundational basis for digital data governance, forming the legal bedrock of user agreements worldwide. However, in practice, consent is often rendered meaningless due to inherent power asymmetries, cognitive manipulation, and the complex nature of digital contracts. Users are frequently compelled to agree to opaque terms and conditions drafted in favor of corporations, raising concerns about whether consent truly reflects autonomy or merely serves as a legal fiction. The digital economy, dominated by private entities with monopolistic control over data, exacerbates this problem by leaving users with little choice but to accept one-sided agreements to access essential services.

In the Indian context, these concerns take on heightened significance due to the country's evolving data protection framework and its vast digital user base, many of whom lack digital literacy. While India's Digital Personal Data Protection Act, 2023 (DPDP Act) attempts to refine consent requirements, its effectiveness is undermined by broad exemptions for state surveillance, weak enforcement mechanisms, and the lack of robust user rights akin to those in the General Data Protection Regulation (GDPR). Given these challenges, legal scholars and policymakers have begun to explore alternative models that move beyond traditional consent-based frameworks.

This paper argues for a paradigm shift from a consent-based approach to an accountability-based model, where corporations must demonstrate data fairness and necessity rather than placing the burden on users to protect their own interests. It examines emerging legal doctrines such as data fiduciary obligations, Digital Habeas Corpus, and data as a human right, proposing stronger legal safeguards to regulate corporate governance in the digital space. Further, this study situates India's evolving data governance framework within a comparative constitutional law perspective, analyzing regulatory approaches in the European Union, Germany, South Korea, and the United States.

Empirical case studies ranging from Aadhaar data leaks and WhatsApp's privacy controversies to Paytm's data-sharing practices illustrate the tangible consequences of weak consent mechanisms and inadequate oversight. Additionally, this paper discusses how artificial intelligence (AI) and algorithmic governance complicate user consent, necessitating bias audits, explainability mandates, and greater transparency in automated decision-making. It also explores how technological and market-based solutions, such as decentralized identity systems and user-owned data markets, can empower individuals in digital transactions.

This study further highlights India's role in G20 digital governance discussions, OECD privacy guidelines, and international data protection frameworks, advocating for a harmonized regulatory approach that balances national sovereignty with global interoperability. Ultimately, this paper contends that a regulatory model based on fairness, accountability, and user empowerment is imperative to replace the inherently flawed concept of contractual consent in digital agreements.

Development and Loopholes in the Consent Framework

In India, user agreements have traditionally relied on contractual consent, a concept rooted in Section 10 of the Indian Contract Act, 1872, which states that agreements entered into freely by competent parties are legally binding. However, digital contracts, including click wrap and browse wrap agreements, create a significant imbalance as users often accept them without a genuine opportunity to negotiate or modify terms. The Information Technology Act, 2000 (IT Act) provides the basic legal framework for electronic contracts, but it does not ensure meaningful consent in cases where users lack the knowledge or bargaining power to make informed decisions.

The DPDP Act, 2023, attempts to strengthen the consent model by requiring explicit and informed consent. However, it contains major loopholes that dilute user protection. First, bundled consent remains prevalent, where users must agree to a wide range of data-processing activities without the ability to selectively opt out. Second, the Act provides broad exemptions for state agencies, allowing government bodies to collect and process personal data without meaningful safeguards, raising concerns about mass surveillance. Third, enforcement remains weak, as the Data Protection Board of India (DPBI) lacks true independence from the executive, limiting its ability to act against non- compliant corporations. Fourth, the Act does not provide adequate protection against algorithmic decision-making, unlike the GDPR, which grants users the right to explanation when automated processes affect them. These gaps highlight the inadequacy of consent as a protective mechanism, necessitating a shift toward corporate accountability and stronger fiduciary obligations.

Private Governance by Corporations and Constitutional Challenges

The power of private corporations in shaping digital rights and governance extends beyond mere contractual arrangements. Technology firms have emerged as quasi-sovereign entities, exercising significant control over privacy, speech, and digital transactions. This phenomenon raises constitutional concerns, particularly in relation to Article 21 (Right to Privacy), Article 19(1)(a) (Freedom of Speech and Expression), and Article 14 (Right to Equality) under the Indian Constitution.

In Justice *K.S. Puttaswamy v. Union of India* , the Supreme Court recognized privacy as a fundamental right, emphasizing that individual autonomy over personal data is central to constitutional governance. However, digital platforms continue to exploit coercive consent mechanisms, effectively privatizing data governance without adequate constitutional oversight.

Similarly, user agreements impact digital free speech, as social media platforms unilaterally determine content moderation policies that can lead to arbitrary censorship without due process. The *Shreya Singhal v. Union of India* ruling, which struck down Section 66A of the Information Technology Act, 2000, highlighted the dangers of vague digital speech restrictions, yet corporations continue to impose restrictions through opaque terms of service.

Furthermore, private governance in digital contracts undermines equality rights, as standard

form contracts drafted by corporations impose one-sided terms on users with no bargaining power. A comparative constitutional analysis reveals that jurisdictions such as Germany, the EU, and South Korea have developed stronger legal doctrines to counterbalance corporate power, offering valuable insights for India's digital regulatory evolution.

Emerging Legal Doctrines

As the inadequacies of consent-based frameworks become increasingly evident, legal scholars have begun advocating for emerging legal doctrines that prioritize user rights over corporate interests. One such doctrine is Digital Habeas Corpus, a concept that enables users to challenge data retention, algorithmic profiling, and opaque decision-making by digital platforms. This doctrine draws parallels with traditional habeas corpus principles, which safeguard individuals from unlawful detention, reimagined in the digital space to challenge unjust data detention and algorithmic discrimination.

Another critical shift is the recognition of data fiduciary obligations, where platforms are legally required to act in the best interests of users rather than merely obtaining consent for data collection. This model, inspired by fiduciary law in corporate governance and trust law, would impose proactive duties on digital platforms to ensure fair data processing, prevent misuse, and disclose algorithmic risks. The California Consumer Privacy Act (CCPA) and GDPR already incorporate elements of such obligations, setting a precedent for India to adopt similar reforms.

Technological and Market-Based Solutions

While regulatory interventions are crucial, technological and market-based solutions also offer promising alternatives to improve user control over digital agreements. The concept of user-owned data markets challenges the current data economy by allowing individuals to negotiate the value of their personal information rather than surrendering it for free. Similarly, decentralized identity systems powered by blockchain and cryptographic verification could replace centralized data storage models, reducing risks associated with data breaches and unauthorized access. AI-driven consent assistants can further help users make informed decisions by summarizing legal agreements in comprehensible language, mitigating the problem of information asymmetry.

Power Imbalance & Autonomy

The principle of consent is grounded in autonomy, yet in practice, digital platforms manipulate users into agreeing to terms that disproportionately favor corporations. This imbalance arises due to cognitive biases, asymmetrical information, and economic constraints. Platforms leverage default settings, deceptive design patterns (dark patterns), and urgency tactics to nudge users into consenting without meaningful deliberation. Moreover, users often lack clarity on how their data will be used, stored, or shared due to legal jargon and excessively long agreements. These factors contribute to a system where consent is not genuinely informed or voluntary, raising concerns about its legitimacy in digital contracts.

Constitutional Challenges

User agreements intersect with several fundamental rights enshrined in the Indian Constitution, particularly the right to privacy under Article 21, the freedom of speech and expression under Article 19(1)(a), and the right to equality under Article 14. The Supreme Court of India in *Justice K.S.*

Puttaswamy v. Union of India, recognized privacy as a fundamental right under Article 21, emphasizing that consent alone cannot justify arbitrary intrusions into personal data. Despite this, digital platforms continue to exploit vague and coercive consent mechanisms, undermining the spirit of this ruling.

Further, user agreements influence digital free speech under Article 19(1)(a). Social media companies and digital platforms implement content moderation policies that can restrict speech arbitrarily, often without transparent justifications or due process. The Indian Supreme Court, in *Shreya Singhal v. Union of India*, struck down Section 66A of the IT Act, holding that vague restrictions on online speech are unconstitutional. However, many user agreements grant excessive discretionary powers to platforms, which can lead to private censorship, a growing concern in digital governance.

Moreover, Article 14 (Right to Equality) concerns arise as large technology corporations draft one- sided agreements that deprive users of bargaining power. The standard form contract model used by digital platforms creates an inherent power imbalance, violating the principles of fairness and equality enshrined in Indian contract law and constitutional jurisprudence.

Ethical Perspectives: Is Consent Sufficient?

Applying ethical theories helps determine whether consent alone justifies data collection and usage. From a deontological perspective, consent should be informed, voluntary, and revocable. If users are manipulated into consenting, the agreement lacks moral legitimacy. On the other hand, a utilitarian approach may justify certain data practices if they yield significant social benefits, such as improved artificial intelligence systems or public health insights. However, such benefits must be balanced against potential harm to individual privacy and autonomy. Ethical considerations suggest that consent alone is an inadequate safeguard, necessitating additional protections such as fiduciary duties for platforms.

Recognizing the limitations of traditional consent models, legal scholars and policymakers have proposed alternative regulatory interventions. One approach is mandated fairness audits, requiring platforms to conduct and disclose assessments that evaluate the impact of their terms on user rights.

Another alternative is the implementation of standardized consumer rights, such as data portability, the right to explanation, and algorithmic transparency, as seen in the European General Data Protection Regulation (GDPR). Additionally, some jurisdictions are shifting towards prescriptive regulations that require privacy-by-design principles, ensuring that default settings favor user protection rather than commercial exploitation.

International Perspective

India's regulatory framework for user agreements and data privacy differs significantly from global models, each with its strengths and weaknesses. The European Union's GDPR prioritizes user autonomy, data subject rights, and explicit consent, making it a stronger protection model than India's DPDP Act, which still lacks comprehensive user rights mechanisms. The United States, in contrast, follows a sectoral approach with laws like the California Consumer Privacy Act (CCPA) and Federal Trade Commission (FTC) regulations, which provide limited consumer protections without a unified federal privacy law.

China's Personal Information Protection Law (PIPL) is stricter than India's DPDP Act, as it mandates data localization and provides stronger enforcement mechanisms. While India's data localization policies align with China's model, enforcement gaps make implementation weaker.

At a global level, India must navigate the complexities of cross-border data transfers, particularly within the frameworks of G20 digital governance initiatives and UN-led discussions on digital rights.

Impact

The reliance on consent-based user agreements has significant negative consequences in India. One of the primary concerns is low digital literacy, particularly in rural and semi-urban areas, where users unknowingly consent to exploitative data-sharing policies. This digital divide worsens the power asymmetry between individuals and large tech corporations, further eroding consumer rights.

Additionally, the prevalence of dark patterns in digital platforms poses a major challenge. Companies use deceptive UI/UX strategies to manipulate users into granting excessive permissions, often in violation of their privacy rights. In India, large digital monopolies like Meta, Google, and Reliance Jio dominate the market, significantly reducing user choice and negotiation power in digital agreements. The lack of robust enforcement mechanisms further exacerbates these challenges, as users have limited legal recourse against unfair terms and conditions.

Recommendations

To move beyond the limitations of consent-based frameworks, India must adopt a fairness and Accountability based model that prioritizes user rights over contractual formalities. First, the DPDP Act should impose stricter obligations on companies to ensure data minimization, purpose limitation, and ethical data processing. Second, regulatory oversight must be strengthened by making the Data Protection Board of India (DPBI) truly independent, ensuring it can proactively regulate digital platforms.

Third, algorithmic transparency must be mandated, requiring companies to disclose automated decision-making processes, especially in AI-driven services like targeted advertising and content moderation . Fourth, alternative dispute resolution mechanisms should be introduced, enabling consumers to challenge unfair agreements through fast-track consumer courts or a public digital ombudsman. Finally, stronger international cooperation is necessary to harmonize Indian data protection laws with global best practices, ensuring cross-border data

security while protecting national sovereignty.

By shifting the focus from mere consent to fairness, accountability, and user empowerment, India can build a more equitable and effective digital rights framework that safeguards citizens from exploitative digital practices.

Bibliography

- *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (India).
- Digital Personal Data Protection Act, No. 30, Acts of Parliament, 2023 (India).
- Information Technology Act, No. 21, Acts of Parliament, 2000 (India).
- Indian Contract Act, No. 9, Acts of Parliament, 1872 (India).
- General Data Protection Regulation, Regulation (EU) 2016/679.
- California Consumer Privacy Act, Cal. Civ. Code § 1798.100 (2018).
- Personal Information Protection Law, Standing Comm. Nat'l People's Cong., 2021 (China).
- **Nandan Nilekani et al.**, *Data Empowerment & Protection Architecture: A Consent Framework for India* (MeitY, 2020).
- **Justice B.N. Srikrishna Committee**, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018).
- **Shoshana Zuboff**, *The Age of Surveillance Capitalism: The Fight for a Human Future at the* Rahul Matthan, *Beyond Consent: A New Paradigm for Data Protection*, 13 Ind. J. L. & Tech. 1 (2017).
- Malavika Jayaram, *Privacy in India: The Emerging Landscape*, 8 Int'l Data Priv. L. 164 (2018).
- Anupam Chander, *The Right to Explanation in India's AI Governance Framework*, 54 Geo. J. Int'l L. 179 (2023).
- Woodrow Hartzog, *The Failure of Notice and Consent as a Privacy Safeguard*, 51 Wash. U.
  J.L. & Pol'y 301 (2016).
- Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 Calif. L. Rev. 671 (2016).
- OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (2013).

- United Nations, *Roadmap for Digital Cooperation* (2020).
- Ministry of Electronics & IT (MeitY), *India's Draft National Data Governance Framework Policy* (2022).
- Nikhil Pahwa, *Explained: How India's DPDP Act Compares to GDPR*, *Medianama* (Aug. 15, 2023), https://www.medianama.com.
- Pranav Dixit, *India's Digital Privacy Debate Heats Up Amid WhatsApp Controversy*, *BuzzFeed News* (Jan. 18, 2021), https://www.buzzfeednews.com.
- Karan Sinha, *Paytm & Data Sharing: What It Means for Indian Consumers*, *The Quint* (Oct. 3, 2022), https://www.thequint.com.
- *Aadhaar Data Leak Exposes Millions*, *BBC News* (July 30, 2021), https://www.bbc.com.