INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

Copyright © International Journal for Legal Research & Analysis. All rights reserved.

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

DATA PROTECTION, PRIVACY AND SURVEILLANCE: A CONSTITUTIONAL AND LEGAL VIEWPOINT

AUTHORED BY - TANVEEN KAUR

Privacy sits right at the heart of modern constitutional democracies. It shapes how people relate to the state and sets the boundaries for how much the government can intrude into someone's personal life. Courts have read and expanded Article 21—the guarantee of life and personal liberty—privacy has become a constitutional right in practice. Technology has changed everything. Now we have digital governance, biometric IDs, artificial intelligence, and massive data collection. People aren't just citizens on paper anymore; they've got digital profiles that decide how they access welfare, services, and even their rights. This shift has created a new kind of power imbalance between the state and the individual. Protecting privacy isn't just about personal freedom anymore—it's become essential for democracy itself.[1]

Article 21 of the Indian Constitution is the bedrock for privacy in India. It guarantees the right to life and personal liberty, and judges have repeatedly stretched its meaning to cover everything a person needs to live with dignity. Articles 14 and 19 also matter— they're about equality and freedom, and they back up privacy, even if not directly.

Indian courts didn't even recognize privacy as a right. In M.P. Sharma (1954) and Kharak Singh (1963), the Supreme Court flat-out said there was no constitutional right to privacy. Still, they admitted there were some protections for personal liberty. Things started to shift with cases like Gobind v. State of Madhya Pradesh (1975), where the Court acknowledged privacy as an implicit constitutional value. The real turning point came with Justice K.S. Puttaswamy v. Union of India (2017). A nine-judge bench unanimously declared privacy a fundamental right under Article 21, making it a core part of the Constitution's protections.

India's data protection laws have grown bit by bit, with sector-specific rules leading up to the Digital Personal Data Protection Act, 2023. This law sets out how personal data should be handled and aims to protect people's information. Still, there are big concerns— especially

[1] V6I150.pdf

about how the law is carried out, the wide exemptions, and the broad surveillance powers the state still holds.

Recognizing privacy as a fundamental right shifts it from just a legal policy to a constitutional duty. It's no longer about protecting physical spaces—it's about giving people control over their own information, choices, and identity. The Supreme Court, especially in the Puttaswamy judgment, made it clear: privacy is tied to dignity, autonomy, and liberty. It's not some special privilege—it belongs to everyone, no matter who they are. In a constitutional democracy, that's a moral foundation.

India's Supreme Court has recognized privacy as a fundamental right, which sounds like a big win. But on the ground, the systems needed to protect that right just aren't there yet. It's not enough to declare privacy a right in theory—you need real ways to enforce it, actual institutions that know what they're doing, and clear lines of accountability. Without these, privacy risks turning into more of a promise than something people actually experience. Right now, the job of protecting privacy mostly falls to executive agencies. These agencies often work behind closed doors, without much independent oversight or real transparency. They're the ones in charge of greenlighting surveillance, collecting data, and sharing information. So, power piles up on the government's side, and ordinary people don't have many options to push back. It messes with the whole idea of checks and balances. Courts are supposed to help, but they usually step in only after the damage is done. The legal system offers relief once a violation happens, but it doesn't do much to stop problems before they start. And in the digital world, once your data is out there, you can't really put the genie back in the bottle. The harm is permanent, which makes prevention way more important than patching things up afterward. India doesn't have a dedicated body to handle privacy issues the way it does for the environment or consumer rights. That means there's no specialized place for people to go when their privacy is threatened. Without this kind of structure, the promise of privacy in the Constitution ends up hollow.

Government is changing fast, and a big part of that shift comes from algorithms and automated systems. These days, governments use algorithms everywhere — handing out welfare, checking IDs, running risk assessments, policing, even making administrative decisions.

Bad data, biases baked into the code, mistakes in the inputs — all of that can mean someone

gets shut out, treated unfairly, or flat-out denied their rights. When a computer starts to replace human judgment, people stop being citizens with rights and just become data points in a system. At the heart of the constitution is the idea that every person has dignity. Reducing people to their data strips that away. Suddenly, citizens start to look more like objects to be managed than individuals with agency and rights. That's not what Article 21 — with its focus on dignity, autonomy, and personal freedom — is supposed to protect.

Surveillance is also the major problem. Algorithms don't just watch what you've done; they try to guess what you might do next. So, the government moves from judging actions to predicting behaviour, operating more on suspicion than on actual evidence. That flips the script on the whole relationship between the state and its people. The presumption of innocence and the rule of law start to look shaky when a computer decides you're risky before you've done anything at all.

Privacy threats these days aren't just about big government watching you. Now, private companies especially tech giants hold more personal data than most governments ever have. They scoop it up, sift through it, and turn it into profit. People call this "surveillance capitalism," and honestly, it's a kind of power that's slipped right past the usual checks and balances you'd expect from the Constitution. These data monopolies don't just sell ads. They shape what you see, what you click, and even what you think—using algorithms and carefully curated content. On the surface, it's all about business. These tactics sway public opinion, nudge elections, and change how society talks to itself. At the heart of the Constitution is the idea that every person has dignity. Reducing people to their data strips that away. Suddenly, citizens start to look more like objects to be managed than individuals with agency and rights. That's not what Article 21 — with its focus on dignity, autonomy, and personal freedom — is supposed to protect.

There are gaps—places where neither constitutional law nor regular regulations keep your privacy safe. As these companies become part of the backbone of daily life, it's clear that privacy protections can't just focus on the government. They need to keep up with this new reality.

Privacy violations hit marginalized communities the hardest. People without much digital know how, those struggling financially, or folks who can't easily fight back legally, they're the

ones most at risk for data abuse and constant surveillance. If you don't really get what companies are doing with your information, you can't give real consent. Those long privacy policies and so called "agreements" end up being a sham when people aren't really choosing—just clicking through because they have to.

Suddenly, Privacy isn't just some abstract right—it's about whether you can get the basics you need to live. So, privacy isn't just something for the privileged to worry about. It's a justice issue. If we want real equality and inclusion, protecting privacy has to be part of the foundation in any democracy that claims to care about social justice.

Digital surveillance is a new kind of government control. Unlike old-school surveillance, where someone was physically followed or watched, digital tools allow the state to monitor people constantly, automatically, and at a huge scale.

Biometric IDs, facial recognition, metadata collection, predictive policing- these systems operate in the background, often without anyone noticing. That sounds solid on paper. But, honestly, putting this into practice is where things fall apart. Laws can be vague, government agencies often have blurry limits, and proper checks are missing.

In the end, these loopholes make constitutional protections feel more like suggestions than real shields.

Observations

1. Privacy has solid backing in the Indian Constitution, but enforcement by institutions is weak.
2. Digital governance is moving faster than privacy protections.
3. Surveillance isn't very open or accountable. This kind of surveillance chills democracy. When people know they're always being watched, they start to hold back. They think twice before speaking, meeting, or moving around freely. Privacy, then, isn't just a luxury—it's vital for keeping democratic participation and free thought alive.
4. Data protection laws talk about rights, but don't offer much in practice.
5. Courts are evolving the doctrine, but the government isn't really following through.

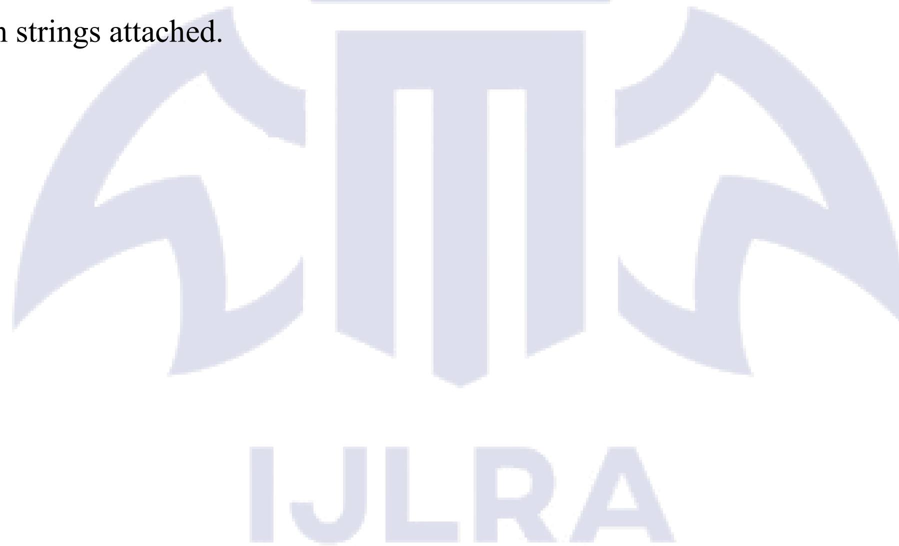
ISSN: 2582-6433

Recommendations

1. Establishment of independent data protection authorities.
2. Strong judicial oversight over surveillance mechanisms.
3. Transparent data governance frameworks.
4. Limitation of blanket exemptions to State agencies.
5. Public accountability mechanisms for digital governance systems.
6. Privacy impact assessments for government technologies.

Conclusion

Recognizing Privacy as a constitutional right was a turning point for India. In a world where data and algorithms hold real power, protecting privacy needs more than good intentions. It needs strong institutions that actually work. Today, privacy isn't just about individuals. It's the backbone of democracy. Without it, freedom is just for show, dignity is hollow, and liberty comes with strings attached.


IJLRA