



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

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal – The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

WHITE BLACK
LEGAL

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 diploma in Public

a professional 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

INTERSECTION OF HUMAN RIGHTS AND **DIGITAL SURVEILLANCE IN INDIA A** **COMPREHENSIVE ANALYSIS**

AUTHORED BY - KISHORE CHANDURU K R

Introduction

Overview of Digital Surveillance

The observation of digital communications and activities through electronic methods is what digital surveillance refers to. The monitoring and gathering of data from electronic communications and activities fall under digital surveillance. This consists of intercepting emails, phone calls, text messages, and online behaviours¹. Advancements in technology have led to more sophisticated digital surveillance, allowing for extensive tracking and analysis of individuals' digital footprints. In India, the development of digital surveillance has followed the worldwide surge in technology, driven by security concerns and the increasing dominance of digital platforms².

Relevance to Human Rights

The convergence of digital surveillance and human rights gives rise to important concerns regarding privacy, freedom of speech, and safeguarding civil liberties. With the advancement of surveillance technologies, there is an increased risk of misuse and exceeding authorized limits, highlighting the need for a thorough assessment of their impact on individual rights. The significance of human rights within the realm of digital surveillance is extensive and diverse, as the digital era has fundamentally transformed the methods through which personal data is gathered, stored, and evaluated³. Human rights, particularly the right to privacy, play a vital role in ensuring that surveillance practices do not violate individual freedoms and civil liberties. With the rising

¹ <https://www.sciencedirect.com/topics/psychology/digital-surveillance>

² https://www.law.cornell.edu/wex/electronic_surveillance#:~:text=Electronic%20surveillance%20is%20the%20acquisition,a%20reasonable%20expectation%20of%20privacy.

³ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418485

use of advanced surveillance technologies by governments and corporations, there is an increasing risk of misuse and excessive intrusion, underscoring the importance of maintaining legal and ethical standards to safeguard personal privacy. The convergence of human rights and digital surveillance emphasizes the necessity of strong legal structures and supervisory measures to weigh national security concerns against the protection of basic freedoms and guarantee that progress in technology does not compromise individual rights.

Historical Context of Surveillance

➤ Traditional Surveillance Techniques

Historically, surveillance in India was conducted through physical means such as wiretapping, mail interception, and physical monitoring. The colonial legacy, including laws like the Indian Telegraph Act, laid the groundwork for later digital surveillance practices⁴. Also, surveillance involved physical methods such as wiretapping, mail interception, and direct observation. These methods were labour-intensive and limited in scope, focusing primarily on targeted individuals or groups.

➤ The Transition to Digital Surveillance

The rise of digital technology revolutionized surveillance, enabling the collection of vast amounts of data with relative ease. The transition from analog to digital methods increased the efficiency and scope of surveillance, making it possible to monitor large populations.

➤ Modern Developments

Today, digital surveillance includes advanced techniques such as data mining, machine learning algorithms, and real-time monitoring. Technologies like facial recognition, geolocation tracking, and internet monitoring have expanded the capabilities of surveillance systems. The advent of digital technology revolutionized surveillance, making it more pervasive and less intrusive in appearance.⁵ The expansion of internet services, mobile networks, and social media platforms has provided new avenues for surveillance and data collection.

⁴ <https://news.harvard.edu/gazette/story/newsplus/surveillance-from-vision-to-data-explores-history-of-surveillance/>

⁵ <https://nap.nationalacademies.org/read/11896/chapter/13>

International Legal Standards

International human rights frameworks, such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights (ICCPR), recognize the right to privacy and freedom from arbitrary interference. These standards provide a foundation for evaluating the legality and legitimacy of surveillance practices⁶.

Key International Agreements and Treaties

Several international agreements and treaties address digital surveillance and privacy issues. For example:

- The Council of Europe's Convention 108 is the only binding international treaty specifically addressing data protection.
- The EU General Data Protection Regulation (GDPR) sets a high standard for data protection and privacy in the European Union.

Legal Framework for Digital Surveillance in India

- The Information Technology Act, 2000

The IT Act governs various aspects of digital communication and data protection. It provides the legal basis for the interception of electronic communications under certain conditions, balancing security needs with privacy considerations⁷.

- The Indian Telegraph Act, 1885

Originally designed for telegraphs, this Act has been adapted to cover modern communication methods. It provides the framework for authorized interception and monitoring, but its application has faced scrutiny in light of contemporary privacy concerns⁸.

- The National Investigation Agency Act, 2008

This Act established the National Investigation Agency (NIA) to handle national security threats,

⁶ <https://privacyinternational.org/sites/default/files/2017-12/Guide%20to%20International%20Law%20and%20Surveillance%20August%202017.pdf>

⁷ <https://www.orfonline.org/expert-speak/the-state-of-surveillance-in-india>

⁸ <https://www.orfonline.org/expert-speak/the-state-of-surveillance-in-india>

including those involving digital communications⁹. It grants extensive powers for surveillance and data collection, raising questions about proportionality and oversight.

➤ The Unlawful Activities (Prevention) Act, 1967

UAPA addresses threats to national security and public order, including those that arise from digital activities. It has been criticized for its broad scope and potential for misuse, particularly in the context of surveillance¹⁰.

➤ Recent Amendments and Legislation

Recent amendments to these laws and the introduction of new legislation reflect the increasing emphasis on digital surveillance. The introduction of the Personal Data Protection Bill is a significant development, aiming to address privacy concerns more comprehensively.

Human Rights and Digital Surveillance

➤ Privacy as a Human Right

Privacy is a fundamental human right recognized under various international treaties and national constitutions. In India, the right to privacy was reaffirmed by the Supreme Court in the landmark K.S. Puttaswamy case, highlighting the need for stringent safeguards against intrusive surveillance¹¹.

➤ Freedom of Expression and Information

Digital surveillance can impact freedom of expression by creating a chilling effect, where individuals may self-censor due to fear of being monitored. This undermines democratic values and the right to free speech¹².

➤ The Right to a Fair Trial and Protection from Arbitrary Detention

Surveillance practices that lead to unjustified detentions or interfere with legal processes can

⁹ <https://repository.nls.ac.in/slr/vol16/iss1/5/>

¹⁰ <https://www.hindustantimes.com/analysis/uapa-when-laws-turn-oppressive/story-d9d7OEO50LQjLZs3Ba5pzI.html>

¹¹ <https://gilc.org/privacy/survey/intro.html>

¹² <https://www.amnesty.org/en/what-we-do/freedom-of-expression/>

violate the right to a fair trial. Ensuring transparency and accountability in surveillance practices is crucial for protecting these rights¹³.

Case Studies and Judicial Perspectives

- K.S. Puttaswamy (Retd.) vs. Union of India¹⁴ (2017)

This landmark case established the right to privacy as a fundamental right under the Indian Constitution. The Supreme Court's ruling emphasized the need for legal safeguards and proportionality in surveillance measures.

- Anuradha Bhasin vs. Union of India¹⁵ (2020)

This case addressed the suspension of internet services in Jammu and Kashmir, highlighting the impact of surveillance and information control on freedom of expression and access to information.

Impact of Judicial Decisions on Surveillance Policies

Judicial decisions have played a critical role in shaping surveillance policies, emphasizing the need for judicial oversight and protection of fundamental rights in the context of national security.

Judicial decisions significantly influence surveillance policies by setting legal precedents and shaping the interpretation and application of laws governing surveillance practices. Courts play a critical role in balancing national security interests with the protection of individual rights, such as privacy and freedom of expression¹⁶. For example, landmark rulings such as the U.S. Supreme Court's decision in *Carpenter v. United States* (2018) established that law enforcement must obtain a warrant to access historical cell phone location data, thereby reinforcing the Fourth Amendment's protection against unreasonable searches and seizures. Similarly, the Indian Supreme Court's judgment in *K.S. Puttaswamy (Retd.) vs. Union of India*¹⁷ (2017) affirmed the right to privacy as a fundamental right under the Indian Constitution, influencing how surveillance

¹³ <https://cja.org/human-rights-issues/arbitrary-detention/>

¹⁴ AIR 2018 SC (SUPP) 1841

¹⁵ AIR 2020 SUPREME COURT 1308

¹⁶ <http://docs.manupatra.in/newsline/articles/Upload/62E569B9-547B-4144-80AC-03A9EBFC45DA.pdf>

¹⁷ AIR 2018 SC (SUPP) 1841

laws must be crafted and implemented to respect this right.

These judicial decisions often lead to legislative reforms, as governments may amend laws to comply with court rulings or address gaps identified by the judiciary. They also provide a framework for evaluating the legality and proportionality of surveillance measures, ensuring that they adhere to constitutional and human rights standards¹⁸. By setting boundaries on the extent and manner of surveillance, courts help prevent potential abuses of power and protect individual freedoms, thereby ensuring that surveillance policies are both effective and respectful of fundamental rights.

Government Surveillance Programs

➤ **The Aadhaar Program**

The Aadhaar program, a biometric identification system, has been controversial due to concerns about data security and privacy. While it aims to streamline services and welfare programs, its implementation raises significant privacy concerns.

➤ **The Central Monitoring System (CMS)**

The CMS is a government initiative designed to monitor telecommunications and internet activities. It operates with limited oversight, raising concerns about the balance between security and individual privacy.

➤ **The National Intelligence Grid (NATGRID)**

NATGRID aims to integrate data from various sources for security and intelligence purposes. Its extensive data collection capabilities have raised concerns about potential misuse and lack of transparency.

➤ **The National Security Agency (NSA) Framework**

The NSA framework involves collaboration with international intelligence agencies and focuses on counter-terrorism efforts. Its surveillance practices must be carefully regulated to ensure

¹⁸ <https://www.orfonline.org/expert-speak/the-state-of-surveillance-in-india>

compliance with human rights standards.

Data Protection and Privacy Concerns

➤ Data Collection and Storage Practices

The collection and storage of personal data by both government and private entities pose significant risks to privacy. Ensuring robust data protection measures is essential to prevent unauthorized access and misuse.

➤ Risks and Vulnerabilities

Digital data is susceptible to breaches, hacking, and misuse. The risks associated with inadequate data protection measures can lead to severe privacy violations and security threats.

➤ Cross-Border Data Transfers and Implications

Global data transfers raise concerns about jurisdiction and data protection standards. Ensuring that data transfers comply with international standards is crucial for protecting privacy.

The Role of Technology Companies

➤ Compliance with Government Orders

Technology companies often face pressures to comply with government surveillance orders. Balancing legal obligations with ethical considerations is a challenge for these companies.

➤ Ethical Considerations and Corporate Responsibility

Technology companies have a role in advocating for privacy and transparency. Ethical considerations include ensuring that surveillance practices do not infringe on individual rights and freedoms.

➤ Transparency and Accountability

Transparency in surveillance practices and accountability for misuse are critical for maintaining public trust and safeguarding human rights. Technology companies must take proactive steps to address these issues.

Civil Society and Activism

➤ Role of NGOs and Advocacy Groups

NGOs and advocacy groups play a vital role in raising awareness about privacy issues and challenging invasive surveillance practices. Their efforts contribute to shaping public discourse and influencing policy changes¹⁹.

➤ Public Campaigns and Awareness Initiatives

Public campaigns aim to educate individuals about their privacy rights and the implications of surveillance. Increasing awareness helps foster a more informed and engaged citizenry²⁰.

➤ Legal Challenges and Reforms

Legal challenges brought by civil society organizations have led to significant reforms and improvements in surveillance policies. Continued advocacy is essential for addressing emerging privacy concerns.

International Perspectives and Comparisons

➤ Global Standards for Digital Surveillance

International standards, such as those established by the UN and other bodies, provide guidelines for balancing security and privacy. Comparing India's practices with global standards helps identify gaps and areas for improvement²¹.

➤ Comparative Analysis with Other Democracies

Examining how other democracies handle digital surveillance provides insights into best practices and potential pitfalls. This comparative analysis can inform policy reforms and strengthen protections.

➤ Lessons from International Jurisprudence

International jurisprudence offers valuable lessons for addressing privacy and surveillance issues.

¹⁹ <https://isd.iss.nl/home/civic-activism/>

²⁰ <https://gsdrc.org/topic-guides/social-exclusion/lessons-and-tools/the-role-of-civil-society-and-social-movements/>

²¹ https://heinonline.org/hol/cgi-bin/get_pdf.cgi?handle=hein.journals/swales37§ion=34

Incorporating these lessons can help enhance India's legal framework and human rights.

Conclusion

In conclusion, the intersection of human rights and digital surveillance in India underscores a critical and evolving area of legal and ethical consideration. As digital surveillance technologies advance, the challenge lies in striking a delicate balance between ensuring national security and safeguarding individual rights. The Indian legal framework, including landmark judgments like *K.S. Puttaswamy (Retd.) vs. Union of India*²², has affirmed privacy as a fundamental right, setting important precedents for how surveillance must be conducted. While surveillance is a necessary tool for modern governance and security, it must be governed by stringent legal safeguards and oversight mechanisms to prevent misuse and protect civil liberties. Moving forward, it is imperative for Indian policymakers to continue refining surveillance laws, enhancing transparency, and ensuring that technological advancements do not come at the expense of fundamental human rights. Strengthening judicial oversight, incorporating public and civil society feedback, and adhering to international human rights standards will be crucial in navigating the complex landscape of digital surveillance while upholding the core values of democracy and individual freedom.

²² AIR 2018 SC (SUPP) 1841