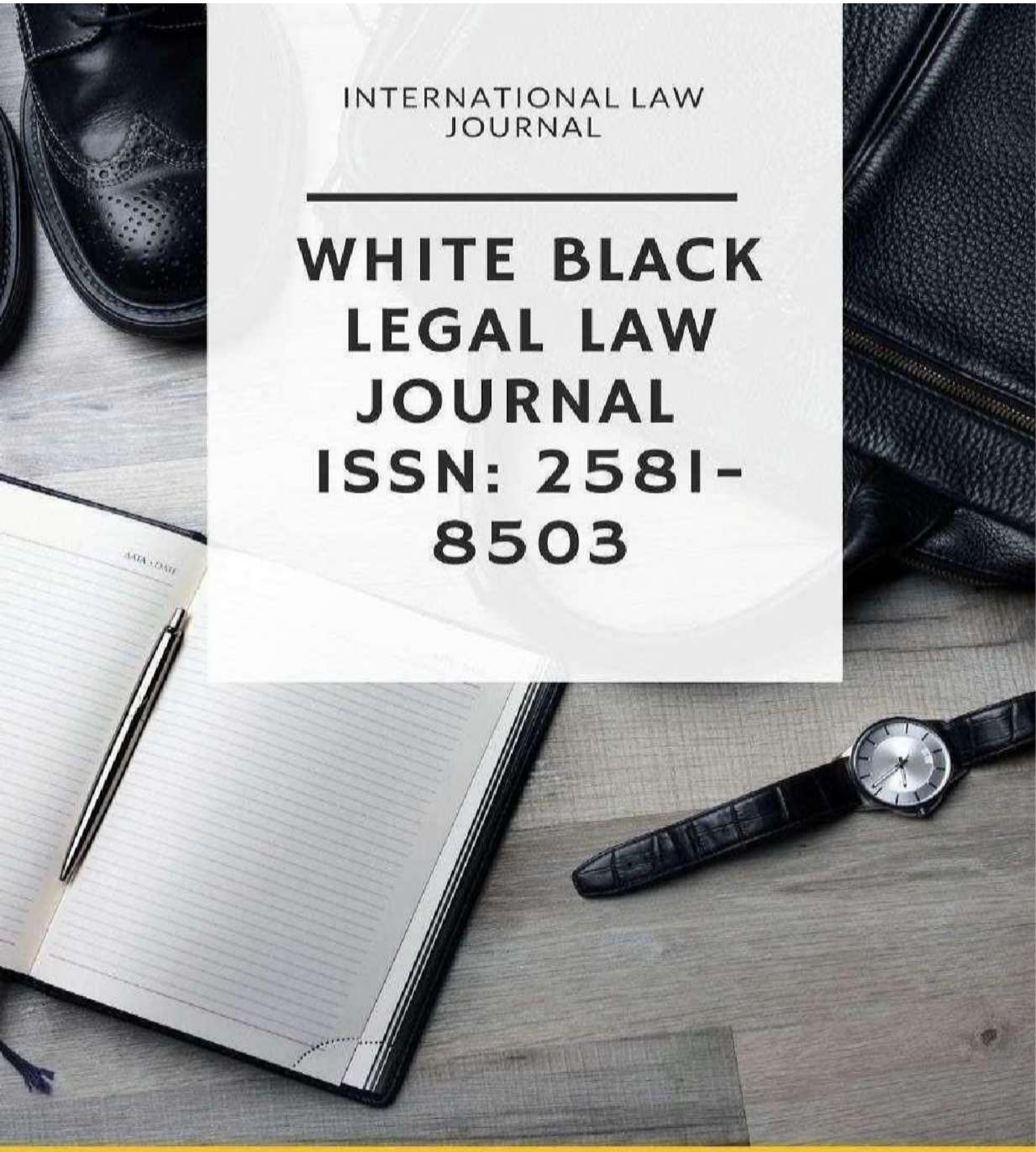

INTERNATIONAL LAW JOURNAL

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.

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

JUDICIAL APPROACH TO PREDICTIVE POLICING AND ELECTRONIC SURVEILLANCE IN INDIA VIS-A-VIS RIGHT TO PRIVACY

AUTHORED BY - *BIKRAM SINGH GORAYA[1]

ABSTRACT

With the technology making inroads in the society, it has shaped every aspect of perception and governance of society. Data and algorithm based technologies e.g. Artificial Intelligence (AI) has altered the landscape of law enforcement mechanism. Mapping the potential hazards of crimes is a measure which has the potential to transform the approach of police forces towards crime. Accompanied by this, is the adoption of electronic surveillance especially digital surveillance which can aid the policing by making it cost saving and better targeting.

Though technology has gained traction in law enforcement and policing initiatives, it has also faced debates and controversies surrounding the use and processing of personal data or information for policing without consent of individuals. The Indian judiciary has played a proactive role in establishing a balance between Right to privacy of individuals vis-à-vis predictive policing and electronic surveillance. The research paper traces the judicial approach of Indian courts in balancing Right to privacy with state interest of crime controlling from the times of physical surveillance and highlights how the judicial approach in digitized world has been shaped by the approach courts adopted in the cases pertaining to physical surveillance.

KEYWORDS Crime controlling Privacy State Interest

I. INTRODUCTION

Predictive policing algorithms (PPAs) refer to the use of technologies in data science and artificial intelligence (AI) to predict threats and suggest solutions in law enforcement. Modern-day police are increasingly turning to big data tools to forecast where and when crimes will occur and who might be

[1] Research Scholar, Department of Laws, Panjab University, Chandigarh.

involved.[2] An act of surveillance always involves the purposeful gathering of information about something or someone. That information is then rationally and systemically analysed and the outcome of that analysis is then used to influence the behaviour of the original surveillance target. For a phenomenon to qualify as surveillant, two elements need to be present: data must be gathered and analysed, and then applied in a process of influence over the original data target. Surveillance always involves an exercise of power.[3] In case the data gathering is done by electronic or digital instruments, the act of surveillance is termed as electronic surveillance. A recent study found that smart technologies such as AI could help cities reduce crime by 30 to 40 per cent and reduce response times for emergency services by 20 to 35 per cent. The same study found that cities have started to invest in real-time crime mapping, crowd management and gunshot detection.[4] Cities are making use of facial recognition and biometrics (84 per cent), in-car and body cameras for police (55 per cent), drones and aerial surveillance (46 per cent), and crowdsourcing crime reporting and emergency apps (39 per cent) to ensure public safety. However, only 8 per cent use data-driven policing. [5]

The judicial approach to predictive policing and electronic surveillance has been shaped according to the changing era of ICTs and its effect on the society. A democratic society thrives by maintain a harmony between its development and societal values. With the advent of ICTs, mankind has experienced development at an unprecedented scale. The technological developments apart from its scalable opportunities, has also been a constant challenge for the society to balance its human rights vis-à-vis technological advancements. Using technologies for predictive policing and electronic surveillance is part of the above trail where it has been an constant challenge for judiciary to establish a harmony between technology used for crime controlling with that of fundamental rights of individuals especially Right to Privacy of individuals. The Indian Judiciary has approached the various conflicts and disputes in policing and surveillance by observing their impact on fundamental rights, by analysing and interpreting the legislative frameworks and by identifying legislative voids.

---

[2] Tzu Wei Hung & ChunPing Yen, *Predictive policing and algorithmic fairness,* 201 Synthese, 206 (2023). DOI: https://doi.org/10.1007/s11229-023-04189-0.

[3] Ball, Kirstie, Electronic Monitoring and Surveillance in the Workplace. Literature review and policy recommendations, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-43340-8, doi:10.2760/5137, JRC125716

[4] Deloitte, Surveillance and Predictive Policing through AI, https://www.deloitte.com/global/en/Industries/government-public/perspectives/urban-future-with-a-purpose/surveillance-and-predictive-policing-through-ai.html. (last visited Feb 21, 2023).

[5] *Id.*

II. PREDICTIVE POLICING AND ELECTRONIC SURVEILLANCE VIS-A-VIS RIGHT TO PRIVACY

In *Kharak Singh's case*[6], Kharak Singh who had been acquitted of dacoity due to lack of evidence, was subjected to surveillance by the U.P. Police under Chapter 20 of the U.P. Police Regulations, and known as the 'history sheet'. This regulation allowed police to monitor individuals considered habitual criminals or likely to become habitual criminals. The surveillance involved secret monitoring of his residence, nightly visits, inquiries about his reputation, habits, associations, income, expenses, occupation, tracking his movements, and keeping records of his activities. Kharak Singh challenged the constitutionality of Chapter 20, arguing that it authorized unconstitutional surveillance by police officials. . The court in this case [7]observed that the regulations were not legislative but executive in nature and henceforth lacking statutory basis and the court articulated that the regulations were neither law under Article 21 as required by the words 'procedure established by law' under Article 21 neither did these regulations satisfies the test laid down under Article 19 of the Indian constitution. It found that clauses allowing surveillance didn't impede physical movement, thus not breaching Article 19(1) (d) or 21. The judgement on this case[8] held (with dissenting of Justice Subba Rao and Jusitce Shah) that the surveillance method of domiciliary visit is violation of Article 21 of the Indian constitution. While the court upheld the remaining clauses, asserting privacy isn't a guaranteed right under the Indian Constitution, the minority view considered privacy essential to personal liberty, advocating for the unconstitutionality of the entire regulation, citing its infringement of Articles 19(1)(d), 19(1)(a), and 21. However, it deemed nightly domiciliary visits (clause b) as infringing Article 21, striking it down.

The writ petition in *Gobind's case*[9] contested the validity of Regulations 855 and 856 of the Madhya Pradesh Police Regulations, which allowed domiciliary visits and other forms of surveillance on individuals with criminal records, under the Police Act, 1961. The petitioner's complaint was that he was labeled a habitual offender due to multiple allegedly false criminal cases against him, leading to the opening of a history sheet and continuous surveillance. He claimed that the police conducted frequent domiciliary visits, secretly monitored his residence, and harassed him. The petitioner argued that such surveillance infringed upon his fundamental rights under Articles 19(1) (d) and 21 of the

[6] Kharak Singh v. State of Uttar Pradesh, (1964) 1 SCR 332 (1962).
[7] *Id.*
[8] *Id.*
[9] Gobind v. State of Madhya Pradesh, (1975)2 SCC 148.

Constitution. The Court while deducing its observation in this case referred and noted the position expounded in the case of *Kharak Singh vs. State of U.P*.[10] and ruled that domiciliary visits under Regulation 236(b) were unconstitutional as held by *Kharak Singh's case*[11] which stemmed from the interpretation of 'personal liberty' under Article 21, which was understood to encompass within itself liberty, freedom, and protection from intrusion within one's own home. The Court specifically referenced Justice K.S. Rao's minority judgment in *Kharak Singh*[12], which recognized the right to privacy within Article 21. Justice K.S. Rao argued that domiciliary visits not only infringed upon the freedom of unrestricted movement under Article 19(1)(d) but also violated the right to privacy, hindering an individual's enjoyment of their rights under Article 21.

"There can be no doubt that privacy-dignity claims deserve to be examined with care and to be denied only when an important countervailing interest is shown to be superior. If the Court does find that a claimed right is entitled to protection as a fundamental privacy right, a law infringing it must satisfy the compelling state interest test. Then the question would be whether a state interest is of such paramount importance as would justify an infringement of the right."[13]

The Court emphasized that privacy and dignity claims should only be rejected if a superior countervailing interest is demonstrated, and any law encroaching on the right to privacy must pass the compelling state interest test. Therefore, the right to privacy can only be violated in pursuit of a compelling and permissible state interest, one that justifies infringing upon a right.

The Bench in the *Malak Singh's case*[14] acknowledged the necessity of striking a balance between the State's objectives of crime prevention and public safety and the constitutional rights enshrined in Article 21 and Article 19(1)(d). It asserted that police surveillance should not encroach upon an individual's personal liberty, dignity, and privacy. While recognizing crime prevention as a legitimate public interest, the Court emphasized that surveillance for this purpose must not constitute an unlawful intrusion into an individual's life. Surveillance activities should be reasonably constrained to allow for the full realization of an individual's fundamental rights. The observations in *Malak Singh* on the issue of privacy indicate that an encroachment on privacy infringes personal liberty under Article 21 and the right to the freedom of movement under Article 19(1) (d). Without specifically holding that privacy is a protected constitutional value under Article 19 or Article 21, the judgment

[10] Kharak Singh v. State of Uttar Pradesh, (1964) 1 SCR 332 (1962).
[11] *Id.*
[12] *Id.*
[13] *Supra* note 12, at 8.
[14] Malak Singh v. State of Punjab and Harayana, (1981) 1 SCC 420 (1980).

of this Court indicates that serious encroachments on privacy impinge upon personal liberty and the freedom of movement. The Court linked such an encroachment with the dignity of the individual which would be offended by surveillance bereft of procedural protections and carried out in a manner that would obstruct the free exercise of freedoms guaranteed by the fundamental rights.[15] The Court therefore articulated and suggested that surveillance would be appropriately limited if it remained discreet, unobtrusive, focused solely on individuals lawfully entered into the surveillance register, and restricted to the objective of crime prevention. Further, the Supreme Court emphasized the significance of crime prevention while underscoring the need for methods to remain within the bounds of personal liberty guaranteed by Article 21 and the freedom of movement under Article 19(1)(d) of the Constitution. It aimed to strike a balance between these interests, asserting that while surveilling habitual or potential offenders might be necessary to prevent organized crime, such surveillance should not excessively infringe upon constitutionally protected freedoms, including the right to privacy.

In *Mr X v. Hospital Z*[16], The Court interpreted the decision in *Malak Singh*[17] as reaffirming the stance on privacy previously established in *Kharak Singh*[18] *and Gobind*[19]. Furthermore, the Court referenced the ruling in *Rajagopal*[20]. It asserted that the right to privacy is not absolute and may be subject to lawful measures aimed at preventing crime or disorder, or safeguarding the health, morals, rights, and freedoms of others.

In the case of *R. Rajagopal v. State of Tamil Nadu*[21], the Court not only broadened the scope of the right to privacy but also advanced it by incorporating the principles of the "right to be let alone" and "safeguarding the privacy of another". In the case of *PUCL v. Union of India*[22], the Court examined the constitutionality of Section 5(2) of the Telegraph Act, which pertains to interception of telegraphic messages. The Court unequivocally recognized that individuals have a privacy interest in the content of their telephone communications, citing previous cases such as *Kharak Singh*[23], *Gobind*[24], *and Rajagopal*[25].

---

[15] Justice K S Puttaswamy (retd.) v. Union of India, (2017) 10 SCC 1.
[16] (1998) 8 SCC 296.
[17] Malak Singh v. State of Punjab and Harayana, (1981) 1 SCC 420 (1980).
[18] Kharak Singh v. State of Uttar Pradesh, (1964) 1 SCR 332.
[19] Gobind v. State of Madhya Pradesh, (1975)2 SCC 148.
[20] R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.
[21] *Id.*
[22] (1997) 1 SCC 301.
[23] Kharak Singh v. State of Uttar Pradesh, (1964) 1 SCR 332.
[24]Gobind v. State of Madhya Pradesh, (1975)2 SCC 148.
[25] R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.

The three important judgements of the era of physical surveillance i.e. *Kharak Singh's case*[26], *Gobind's Case*[27] *and Malak Singh's case*[28] shaped the interpretation of law enforcement measures by law enforcement machineries vis-à-vis right to privacy of individuals. These judgements laid down the groundwork for envisioning technological measures for law enforcement vis-à-vis fundamental rights of individual citizens, which is evident in the subsequent two landmark judgements of *PUCL v. Union of India*[29]*and Puttaswamy judgement*[30].

The present guidelines regulating mass surveillance is vastly influenced by guidelines set in PUCL.[31] With the advancement of sophisticated information and communication technologies (ICTs) such as Telephone; surveillance entered into altogether into a new era and space. Telephone surveillance replaced the need to physical entered into people's home, office and lives. The right to confidential telephone conversations within one's home or workplace is increasingly at risk of exploitation and is susceptible to privacy breaches of individuals. While it's acknowledged that governments, even those with democratic principles, engage in covert intelligence activities for maintaining law and order in the country, citizens' privacy rights must be safeguarded from potential misuse by current authorities. In response to the issue of telephone tapping, the People's Union of Civil Liberties (PUCL), a voluntary organization, had filed a petition in the public interest under Article 32 of the Indian Constitution. This petition challenges the constitutional validity of Section 5(2) of the Indian Telegraph Act, 1885, or alternatively advocates for the inclusion of procedural safeguards to prevent arbitrary and indiscriminate telephone surveillance. This petition filed by PUCL in response to a report published by the Central Bureau of Investigation regarding the tapping phones which revealed numerous procedural deficiencies in the phone tapping carried out by Mahanagar Telephone Nigam Limited (MTNL) at the behest of government officials.

The Court drew its observations in this case[32] by relying upon the earlier judgments in cases such as *Kharak Singh's case*[33], *Gobind case*[34], *and R. Rajgopal case*[35] to establish that while the Indian Constitution does not explicitly state a right to privacy, it is inherent within the right to "life" and

---

[26] Kharak Singh v. State of Uttar Pradesh, (1964) 1 SCR 332 (1962).
[27] Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148.
[28] **Malak Singh v. State of Punjab and Harayana, (1981) 1 SCC 420 (1980).**
[29] People's Union of Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301 (1996).
[30] Justice K S Puttaswamy (retd.) v. Union of India, (2017) 10 SCC 1.
[31] Shruti Singh et al., "*Invasion Of Privacy Through Search and Seizure of Electronic Media: Comparative Study of USA and India"*, 7 *BiLD L. J.*124, 125 . https://bildbd.com/index.php/blj/article/view/49.
[32] People's Union of Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301 (1996).
[33] Kharak Singh v. State of Uttar Pradesh, (1964) 1 SCR 332 (1962).
[34] Gobind v. State of Madhya Pradesh, (1975)2 SCC 148.
[35] R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.

"personal liberty" under Article 21. It emphasized the viewpoint that telephone conversations conducted in private settings constitute a form of privacy, protected under Article 21, and thus, interception through telephone tapping must adhere to established legal procedures. Additionally, the Court recognized telephone conversations as an exercise of freedom of speech and expression under Article 19(1)(a), with interception being subject to reasonable restrictions under Article 19(2).

The Supreme Court maintained that the right to privacy itself has not been expressly enumerated in the Constitution. It suggested that as a concept, privacy might be too broad and subjective to be judicially defined. However, the determination of whether the right to privacy has been claimed or infringed upon in a specific case would rely on the circumstances of that case. Nevertheless, the Court emphasized that the right to engage in a telephone conversation in the privacy of one's home or office without interference can indeed be considered a fundamental aspect of the right to privacy. Telephone conversations often involve intimate and confidential matters and are integral to modern life, as evidenced by the widespread use of mobile phones. Therefore, the right to privacy inherently encompasses telephone conversations conducted in private settings. The Court concluded that telephone tapping would constitute a violation of Article 21 of the Constitution of India, which guarantees the right to life and personal liberty, unless it is authorized under a legally established procedure.

With regard to Section 5(2) of the Act, the Court observed that emphasized that interception orders must meet specific conditions and surrounding factors including the occurrence of a public emergency or interest of public safety, as well as being necessary for the preservation of sovereignty, security, friendly relations with foreign states, public order, or the prevention of incitement to commit an offense. The authorized officer must record reasons in writing before issuing such orders.

While the Court in this judgement[36] declined to declare Section 5(2) unconstitutional, it stressed the importance of strictly adhering to the statutory prerequisites and grounds outlined in the provision. Accompanying and together with this, it rejected the petitioner's proposal for prior judicial scrutiny before interception orders which the petitioner regarded and wanted to deduce as a procedural safeguard, stating that the power to establish rules rests with the Central Government under Section 7 of the Act. Also, the Court criticized the government for failing to enact proper laws despite the widespread criticism of Section 5(2). The significant problem of a public authority’s mass projects of mass surveillance, including the Centralised Monitoring System, is that there is no particular

[36] People’s Union of Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301 (1996).

legislation which backs up such mass surveillance.[37]

To prevent arbitrariness in the implementation of power under Section 5(2) of the Act, and until the Central Government establishes a just, fair, and reasonable procedure under Section 7(2) (b) of the Act, the court in this case[38] conveyed that it is imperative to establish procedural safeguards for the exercise of power under Section 5(9) of the Act. This ensures the protection of an individual's right to privacy. Therefore, the court provided for certain procedural safeguards until government framed comprehensive legislation against arbitrary interception. These safeguards were as follows:-

1. Under Section 5(2) of the Act, an order for telephone tapping may only be issued by the Home Secretary of the Government of India (Central Government) or the Home Secretaries of the State Governments. In urgent situations, this authority may be delegated to an officer of the Home Department of the Government of India or the State Governments, provided they hold a rank not lower than Joint Secretary. Additionally, a copy of the order must be sent to the relevant Review Committee within one week of its issuance.
2. The order issued under Section 5(2) shall mandate the recipient to intercept, during their transmission via a public telecommunication system, the communications specified in the order. Additionally, the order may stipulate that the recipient disclose the intercepted material to designated individuals and in accordance with the instructions provided in the order.
3. In evaluating the necessity of an order under Section 5(2) of the Act, factors to consider include whether the information deemed essential to acquire could reasonably be obtained through alternative means.
4. The interception mandated by Section 5(2) of the Act pertains to communications sent to or from addresses specified in the order, which belong to an address or addresses likely to be utilized for transmitting communications to or from a particular individual specified or described in the order, or to a particular set of premises outlined in the order.
5. The order issued under Section 5(9) of the Act shall expire at the end of a two-month period from its issuance unless renewed. The authority that issued the order, typically the State Government, may renew it at any time before the end of the two-month period.

(a) Within two months of the order's issuance, the Committee shall independently investigate whether there is or has been a relevant order under Section 5(2) of the Act. If such an order exists,

[37] Shruti Singh et al., "*Invasion Of Privacy Through Search and Seizure of Electronic Media: Comparative Study of USA and India"*, 7 *BiLD L. J.*124, 128 . https://bildbd.com/index.php/blj/article/view/49.
[38] People's Union of Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301 (1996).

the Committee examines whether there has been any violation of the provisions of Section 5(2).

(b) If the Committee finds a violation of the provisions of Section 5(2), it shall invalidate the order under review and direct the destruction of intercepted material copies.

(c) If the Committee determines that there has been no contravention of the provisions of Section 5(2), or if it deems it necessary to continue the order, the total period for the operation of the order shall not exceed six months.

6. The authority responsible for issuing the order must maintain the following records:

(a) Records of intercepted communications.

(b) Documentation regarding the extent to which the intercepted material is disclosed.

(c) Information about the number of individuals and their identities to whom any of the intercepted material is disclosed.

(d) Details on the extent to which the intercepted material is copied.

(e) Records indicating the number of copies made of any of the intercepted material.

7. The utilization of intercepted material must be restricted to the minimum extent necessary as outlined in Section 5(2) of the Act.

8. Every copy produced of any intercepted material must be promptly destroyed once its retention is no longer essential in accordance with Section 5(2) of the Act.

9. A Review Committee at the Central Government level shall comprise the Cabinet Secretary, the Law Secretary, and the Secretary of Telecommunications. At the State level, the Review Committee shall include the Chief Secretary, the Law Secretary, and an additional member appointed under Section 5(2) of the Act. If the Committee finds a contravention of the provisions of Section 5(2) of the Act, it shall document its findings accordingly.

The Supreme Court's understanding of privacy, initially tested in cases like *M.P. Sharma*[39] and *Kharak Singh*[40], has progressed to recognize it as an integral aspect of "personal liberty" under Article 21 of the Constitution. The Court has emphasized that while this right isn't absolute, any infringement must meet the standard of being "just, fair, and reasonable". The application of this standard, along with other judicial review criteria, particularly in cases involving state intrusion into privacy, was extensively discussed in the *Puttaswamy case*[41].

[39] M.P. Sharma v. Satish Chandra, (1954) 1 SCR 1077.
[40] Kharak Singh v. State of Uttar Pradesh, (1964) 1 SCR 332 (1962).
[41] Justice K S Puttaswamy (retd.) v. Union of India, (2017) 10 SCC 1.

III. ROLE OF *PUTTASWAMY JUDGEMENT*

The judgement of *Justice K.S. Puttaswamy case* [42] (hereafter referred to as 'The judgement') laid down the sacrosanct principle of Right to privacy as a constitutionally protected value under Constitution of India. "Privacy, with which we are here concerned, eminently qualifies as an inalienable natural right, intimately connected to two values whose protection is a matter of universal moral agreement: the innate dignity and autonomy of man."[43]

"Privacy, in its simplest sense, allows each human being to be left alone in a core which is inviolable. Yet the autonomy of the individual is conditioned by her relationships with the rest of society. Those relationships may and do often pose questions to autonomy and free choice. The overarching presence of state and non-state entities regulates aspects of social existence which bear upon the freedom of the individual." [44]

In the Indian context the judgement said that a fundamental right to privacy would cover at least three aspects or scenarios such as-

- Privacy that involves the person - This is to say that when there is some invasion by the State of a person's rights relatable to his physical body e.g. the right to move freely;

- Informational privacy – informational privacy is one which does not deal with a person's body but deals with a person's mind, this lays down that that an individual may have control over the dissemination of material that is personal to him. Unauthorised use of such information may lead to infringement of this right and lastly

- Privacy of choice-It protects an individual's autonomy over his/her fundamental personal choices.

The Supreme Court has clarified that the right to privacy, much like other fundamental rights, is not absolute. It can be overridden by competing state and individual interests, subject to certain tests and benchmarks. The majority of judges in this decision have agreed to apply the European standard of proportionality to evaluate privacy infringements in the future. However, the application of this doctrine will vary depending on the specific competing interests involved and will evolve on a case-

[42] *Id.*

[43] *Id.* at 321.

[44] *Id.* at 5.

by-case basis. At a minimum, any challenged action will be assessed based on the "just, fair, and reasonable" standard established under Article 21 of the Constitution.

The Supreme Court in this judgement drew the contours of surveillance and predictive policing via profiling in the technological age particularly digital space. Justice Sanjay Kishan Kaul in the *Puttaswamy judgement*[45], highlighted the interface between privacy and technology with the changing times and their impact on surveillance by state actors such as law enforcement strategies with the introduction of digital technologies. In today's information age, technology has greatly expanded access to information, offering numerous benefits but also presenting certain drawbacks. The protection of privacy is crucial, especially regarding access to information that individuals may not wish to disclose. The right to privacy is asserted not only against the State but also against non-state actors, which may necessitate legislative intervention for enforcement. The advancement of technology has provided new avenues for potential privacy infringements by the State, including surveillance, profiling, and data collection and processing.

While surveillance is not a new concept, technological advancements have enabled surveillance methods previously unimaginable. Instances such as Edward Snowden's revelations have brought global attention to the extent of surveillance activities conducted by states, particularly in response to heightened concerns about terrorism and public safety. One method increasingly utilized by states is profiling, defined as automated processing of personal data to evaluate various personal aspects of individuals. Profiling has the potential to lead to discrimination based on factors such as religion, ethnicity, and caste. However, it can also serve public interest and national security objectives. The prevailing security environment, both domestically and internationally, necessitates a delicate balance between ensuring the safety of individuals and the State and upholding the right to privacy. Finding this balance is essential in navigating the complexities posed by evolving technological capabilities and security imperatives. [46] Therefore, privacy cannot have an overriding effect on surveillance every time as both predictive policing via profiling and electronic surveillance for law, peace and national sovereignty, security and integrity are at par or in certain cases more valuable than individual privacy and autonomy.

In order to balance the role of state actors vis-a-via privacy of individuals in a democracy, the judgement deduced a proportionality test to achieve a coherence between privacy and surveillance. This test not only provides a framework for judicial review of the surveillance measures but also is a

[45] Justice K S Puttaswamy (retd.) v. Union of India, (2017) 10 SCC 1.
[46] See also. Justice K S Puttaswamy (retd.) v. Union of India, (2017) 10 SCC 1, at 503.

guiding beacon for states to align their surveillance in accordance with the proportionality principles. An invasion of life or personal liberty must meet the three-fold requirement of (i) legality, which postulates the existence of law; (ii) need, defined in terms of a legitimate state aim; and (iii) proportionality which ensures a rational nexus between the objects and the means adopted to achieve them. [47] Therefore, the action must be sanctioned by law; the proposed action must be necessary in a democratic society for a legitimate aim; the extent of such interference must be proportionate to the need for such interference; and there must be procedural guarantees against abuse of such interference.[48]

Furthermore, the judgment outlined circumstances where restrictions on the right to privacy may be justifiable, subject to the principle of proportionality:

(a) Other fundamental rights: The right to privacy must be weighed against its role in society and balanced against other fundamental rights.

(b) Legitimate national security interest.

(c) Public interest, including scientific or historical research purposes or statistical purposes.

(d) Criminal Offences: The necessity for competent authorities to prevent, investigate, and prosecute criminal offenses, while ensuring safeguards against threats to public security.

(e) The unidentifiable data: Information that does not pertain to identified or identifiable individuals but remains anonymous. The European Union Regulation[49] mentions 'pseudonymisation,' where personal data is processed in a manner that it cannot be attributed to a specific data subject without additional information, which is kept separately and subject to technical and organizational measures to prevent attribution to an identified or identifiable natural person.

(f) Tax and financial regulations: The regulatory framework of taxation and financial institutions may require the disclosure of private information. However, this does not justify disclosing information to everyone, and there should be data protection rules aligned with the objectives of processing. Processing may be permissible if compatible with the purposes for which the information was initially collected.

Therefore, the judgement lays down a comprehensive vision for surveillance and predictive policing in the digital India strengthening its democratic values together with building a strong law enforcement mechanism.

---

[47] *Id.* at 264.

[48] *Id.* at 534.

[49] The European Parliament and of the council Regulation (EU) 2016/679 (General Data Protection Regulation), 2016 O.J. (L 119).

Similarly, following *Puttaswamy judgement*[50], in the case of *Manohar Lal Sharma v. Union of India*[51], the Supreme Court of India examined allegations of privacy breaches involving the use of spyware, particularly the Pegasus suite by NSO Group. The Court acknowledged that surveillance, whether by external agencies or the State itself, encroaches upon citizens' right to privacy. It recognized that while the right to privacy is not absolute, the State may intrude upon it if the measures used pass constitutional scrutiny, referring to the legality, necessity, and proportionality test established in the *K.S Puttaswamy vs. Union of India case*[52]. In the current era of the "information revolution," where individuals' entire lives are stored in digital dossiers, the Court emphasized the need to recognize both the potential for technology to infringe on privacy and its capacity to enhance lives. The Court asserted that in a democratic nation governed by the rule of law, indiscriminate surveillance and spying of individuals cannot be tolerated, and the right to privacy must be appropriately balanced against legitimate security concerns.

IV CONCLUSION

The Supreme Court of India has been a guiding beacon for the country. It has strengthened right to privacy as a fundamental right along its journey of laying down the contours of surveillance. Though it has managed to establish a coherence between fundamental rights and technological advancement but the pace and ambiguity around technology has always been a challenge for the courts. The way forward lays in a holistic approach that assimilates the coordination of all stakeholders of society in order to establish a sustainable technological world.

[50] Justice K S Puttaswamy (retd.) v. Union of India, (2017) 10 SCC 1.
[51] AIR 2021 SC 5396.
[52] (2017) 10 SCC 1.