RES MILITARIS Social Science Journal

"Government Surveillance and Article 19(1)(a): The Law Enforcement in Digital Age: A close Inspection on the legal boundaries"

Sharwan Singh, Vir Vikram Bahadur Singh

Faculty of Juridical Sciences, Rama University, Mandhana, Kanpur. U.P. India

Email id: sharawan.edu@gmail.com

Abstract

In this paper, we will discuss the changing function of government surveillance in India, particularly within the context of digital development and the constitutional guarantees of freedom of speech and expression. Along with the governments acquiring more powers through the use of technology to augment their intervention in law enforcement and maintenance of public order, concerns about the right to privacy and human liberties get more significant. Referring to this article we are going to examine whether these practices support or over rangers Article 19(1)(a) of the Indian Constitution which guarantees citizens' right to freedom of speech and expression. This research reveals the well-organized set of surveillance methods like wiretapping, internet monitoring, and the use of artificial intelligence and facial recognition technology which prove to be the real threat to civil liberties. The legal accord that strictly controls the issue of surveillance, for instance, the Indian Telegraph Act and the Information Technology Act, are evaluated to verify the effectiveness in balancing state security interests against privacy rights. In addition the paper looked at several judicial verdicts which shape the interpretation of Article 19(1)(a), considering the Supreme Court's duty in deciding what is legally permissible. Besides, the paper gives the example of surveillance overreach, which shows the possibility of government intrusion into the private life of the people and the consequent impact on individual freedom. By applying a comparative analysis against IDPS such as the GDPR, the study exhibits a variety of global political scoring mechanisms and guards civil rights. The key is this paper is to make suggestions for legal reforms as well as government policies to ensure that government surveillance will not be abused. The proposed reforms are based on the principles of legality, necessity, and proportionality. Hence, they are designed to protect the fundamental rights and freedoms while at the same time dealing with the national security concerns in the digital era in India. The study ends with the recommendations like to increase transparency, to make court control better and to change legal laws to be equal with new technological facts.

Key Words: Constitutional rights, Digital Privacy, Judicial Oversight, Civil liberties, Technological Advances etc.

1. Introduction

1.1 Background

The digital era has observed up growth of government surveillance such as AI technology catered with deep root of data mining. Governments defend against the use of these techniques by saying terrorism deterrence, crime prevention and ensuring public safety as reasons. Nevertheless, the extensive use of digital surveillance has of late become the major talking point in the debates on privacy, freedom, and the laws which govern these activities. With the presence of Internet and the digital communication technology, the intelligence agencies it is possible to instantly gather, analyze and track down any person of interest within a very short period of time. Surveillance now means more than just infra-red video cameras that are armed with facial recognition and drones, wired-tap along with access to third-party data of telecommunications and internet-service providers[8]. Metadata analysis is a process which can reveal the minutes elements about an individual's contacts, locations, and habits without even listening to the content of communications.

The presence of such extensive surveillance systems complies with the problem of civil rights where two issues stand out especially, privacy and freedom of expression. In India, as these rights are constitutionally guaranteed under Article 19(1)(a) of Indian Constitution, every citizen has the right to freedom of speech and expression which is ensured to them. However, this basic right is not absolute and is under reasonable restrictions when certain conditions are specified. The conflict that might arise between the government surveillance and the Article 19(1)(a) is unique and noteworthy as state surveillance may create a strong obstacle to the provision of human rights. So far, the Supreme Court of India has played the key role doing the interpretation of Article 19(1)(a) on the basis of challenges arising in the digital age. The Court has always placed the emphasis that every violation of privacy must be made in accordance with the conditions of lawfulness, legitimacy, and proportionality. The government is exploiting these

[8]Kashyap, Importance of Freedom of Press under the Ambit of Article 19(1) (A) of the Indian Constitution, 12 Int'l J. Sci. & Res. (IJSR) 1538 (Nov. 5, 2023).

technologies forlaw enforcement and national security; therefore, a balanced stance that considers both security and constitutional rights becomes the priority.

1.2 Objective of the Paper

The objectives of this paper are to:

- **Examine Legal Boundaries:** Analyze the existing legal systems in India that deal with government surveillance and its compatibility with the constitutional provisions, especially Article 19(1)(a). This is a complete look into the acts that govern surveillance, cases that explain it as well as guidelines issued by different forms of administration that regulate the powers of surveillance.
- **Assess Impacts on Civil Liberties:** Conduct the investigation on ways the government surveillance caused civil liberties to be violated through the example of the violation of the freedom of speech and expression. This implies that the issues such as the cases when the surveillance had gone over the legal boundaries, resulting in the violation of the privacy and expression are to be addressed.
- **Evaluate Regulatory Effectiveness:** Critically reflect on how good regulations can be to limit government surveillance (control and regulation) which in turn includes reviewing if there are adequate surveillance mechanisms, the jurisdiction of the judiciary and the transparency of surveillance operations.
- **Recommended Improvements:** Identify the laws and policies that need to be changed to make the government surveillance responsible, that is, to follow the principles of legality, necessity, and proportionality, so that the elementary rights and freedoms are protected.
-

1.3 Significance of the Study

The research explores the detailed nature of government surveillance in India to find out the consistency of the surveillance practices with the constitutional freedoms, more specifically, Article 19(1)(a) which guarantees the freedom of speech and expression. Through digital development, the government's ability to spy on people is enhanced, including wiretapping and

AI-related technologies, and this paper reviews the existing legal frameworks, for example, the Indian Telegraph Act and the Information Technology Act, to determine their efficiency in protecting the privacy of people and at the same time to support the security of the state. Through the paper the scholars illustrate the different judicial interpretations and propose a reform that can be taken to improve policy so that the technology used for surveillance will not violate the civil liberties.

1.4 Research Questions:

This research aims to address several critical questions:

1) How do the current legal systems in India control government surveillance, and do these legal frameworks are compliant with the constitutional provisions, especially Article 19(1)(a)?
2) How can we see that the government surveillance has in some ways intruded upon the civil liberties, especially the freedom of speech and expression?
3) Is the current regulatory system working to the extent of limiting government surveillance in a way that is legal, necessary and proportionate?
4) Which changes can be introduced to the laws and policies in order to avoid the illegal use of surveillance technology and to safeguard essential rights?

2. Review of Literature

The new digital age government surveillance has created complicated legal and ethical problems, especially in relation to Article 19(1)(a) of the Universal Declaration of Human Rights, which states the right to freedom of expression.

This literature review is designed to review the key points of the legal limitations of the police in the area of government observation, by the research findings.According to Solove (2022) the digital age has made the government surveillance process complex, and the pile up of massive amounts of personal data is now possible[8].

[8]Daniel J. Solove, the Digital Person (2022).

This has the main consequences on personal privacy and the freedom of expression, since the boundaries of the surveillance activities are no longer clear. Manning (2019) argues that big data policing is on the rise, where surveillance, race and the future of law enforcement are in a new state of intersection[8]. The application of big data in policing is the cause of the grievance of the discriminatory practices and the possible violation of civil liberties, especially in the marginalized communities. Apart from that, Manning (2019) stresses the necessity of the legal and ethical analysis of the government surveillance, especially the protection of the basic rights, like freedom of expression. The author stressed the need for the surveillance activities to be within the legal limits and respect human rights. Mandelblatt et al. (2016) show how collaborative modelling of the benefits and harms of different surveillance strategies, especially breast cancer screening is studied[8]. Although the study is about healthcare surveillance, the results highlight the general ethical implications that are related to the government surveillance, especially the pros and cons of the safety and the rights of the individuals.

3. Government Surveillance: Scope and Methods

Technology development in the field of government surveillance follows a multitude of directions, including the deployment of not less complicated techniques, which result in exhaustive surveillance and data collection. Here is an overview of the primary surveillance techniques currently employed:

i. **Wiretapping:** Barely, wiretapping alternatively implies the interception of telephone and internet chats. This is done by the law enforcement agencies under legal power to listen to calls and messages to obtain intelligence and evidence against the criminals and potential security threats. It is possible to take the wiretaps for both landline and mobile communications, and usually the detections keep on changing together with telecommunications providers.

[8]P. Manning, The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement, 48 Contemp. Soc. 170 (2019).

[8]J. Mandelblatt et al., Collaborative Modeling of the Benefits and Harms Associated With Different U.S. Breast Cancer Screening Strategies, 164 Annals Internal Med. 215 (2016).

ii. **Internet Monitoring:** It allows the surveillance of all online activities (such as browsing history, emails, social media messages etc.,) such as the digital part of individuals' communications. Internet monitoring equipment can be used to analyze data flow to and from the targeted computers and smart phones; this helps agencies to collect huge amounts of information. The approach that uses deep packet inspection allows the governments to inspect all data which may contain personal information, habits, preferences, as well as locations to highlight the content of communication.

iii. **Artificial Intelligence (AI):** AI technologies are nowadays widely used for area monitoring and data processing automation as well as for the detection of use patterns. AI can analyze huge volumes of data that are beyond human ability, spotting patterns and oddities that may be signs of illegal or suspicious activities[8]. AI systems assist with predictive policing, an analytic tool which helps foresee criminal activity based on historical information and other inputs.

iv. **Facial Recognition Technologies:** This technology, known as facial recognition, studies the shape and the texture of faces observed on the pictures or the videos, in attempts to identify people. It is the most popular and it is used in public security systems in crowded places such as airports, railway stations and city centres. A facial recognition capability could latch on to the identification databases to become a power synthesis tool for surveillance and identification of individuals in real-time.

v. **Use of Drones and Aerial Surveillance:** Drones equipped with cameras and other sensors are deployed to avoid being noticed and for aerial surveillance on large areas by an over viewing camera. This method is applicable for border security, crowd monitoring during events, and in the field of disaster management. Drones that benefit from their manoeuvrability and intrusion level when compared to human needs on the ground get on top the list of much needed surveillance modalities.

3.1 Legal Frameworks Authorizing Surveillance

[8]B. Pandey, Review Article- The Supreme Court and the Constitution: An Indian Discourse, SSRN Electronic J. (2020).

In India, the set of laws authorizing the government surveillance entity is grounded in various acts, which are mainly aimed at protecting the country's security interests and the privacy rights of individuals simultaneously. In this article, I will describe these frameworks and compare them with the global standards.

Indian Legal Frameworks

a) **Indian Telegraph Act, 1885:** This is an old process, which allowed in the "event of any public emergency" or "for the safety and security of the public" hearing on the telegraphic communications of the government. “It is no longer limited to text messages but has also been extended to voice calls and data transmitted over the internet.
b) **Information Technology Act, 2000 (IT Act):** The IT Act which is amended in 2008, deals with e-commerce as well as cybercrime, with additional provisions that allow for the surveillance and monitoring of digital communications. 69(1) of the IT Act enables the central and state government to seek for an interception; monitoring or cracking of data exchanged through computer resource where doing so is desirable for security of the State, friendly relations with foreign states, public order or such other interests including those related to the sovereignty of India[8].
c) **Personal Data Protection Bill, 2019:** The new legislation that will soon be enacted assists the Government in establishing a framework that will respect privacy and enable data processing for legal purposes, such as government functions where the processing of personal data is done without the consent of individuals for the purpose of national security and public order.

Global Standards

[8]R. Kohli, Expressive Conduct and Article 19(1)(a) of the Indian Constitution: A Purposivist Approach, 16 Asian J. Comp. L. 259 (Oct. 12, 2021).

Comparatively, global surveillance laws often include more stringent oversight and transparency mechanisms:

a) **USA PATRIOT Act and Foreign Intelligence Surveillance Act (FISA) in the United States:** This restriction permits any broad surveillance powers with strict controls, but the checks on the sources should be by courts and congress. FISA is just an example in this case, which means that the government has to secure an approval of a judge for conducting electronic surveillance for the purpose of foreign intelligence.
b) **General Data Protection Regulation (GDPR) in the European Union:** GDPR is a very strict regulation that ensures protection of personal data and privacy, including a detailed procedure on the collection and processing of such data. Although it is made to pursue national security goals within the framework of the member states, these activities are generally subject to judicial oversight which may mean that authorities of the member states are required to get court orders before advancing with eavesdropping or any other surveillance operations.
c) **Investigative Powers Act, 2016 (UK):** A "Big Brother" legislation, it indicates measures for gathering the communications information en masse. Nevertheless, it is performed only in exceptional circumstances, such as obtaining warrants for the intrusive surveillance with an independent commissioner doing the supervising.

3.2 Cases of Surveillance Overreach

Government observation, despite being important for the national security and the law enforcement, can sometimes exceed the legal and ethical limits, which ultimately leads to the violation of the law and the civil rights. Here are examples from different contexts where surveillance overreach has raised concerns:

India

a) **The Puttaswamy Case (2017):** This landmark judgment of the Supreme Court of India said that the privacy is just one aspect of the rights and freedom which are ensured under the Indian Constitution. The case description includes the worries over the Aadhaar system equipping the government apparatus with double and triple data and information

of the public. The opponents claimed that there would be no security measures for the Aadhaar system and thus it would cause surveillance and privacy breaches on an unprecedented scale. The decision of court focused on the vein for proportional monitoring and formulating conditions in cases where law is not strong enough to bind the Aadhaar and other surveillance instruments to avoid overreach—highlighting such cases[8].

b) **Phone Tapping Scandals:** In the past, many events in India have occurred with similar circumstances where the agencies were found secretly taping phones without the proper authorization and the exceeding of the given mandate. In most cases, these incidents were related to the tracking of political figures, journalists, and activists, which resulted in a number of important questions about the abuse of surveillance for political instead of security purposes.

International Examples

a) **United States- NSA Surveillance (Snowden Revelations, 2013):** Edward Snowden, a former contractor of the NSA, dumped a huge number of documents that exposed that the NSA has-been recording and storing phone messages and Internet communications all over the world for a long time. Such surveillance takes place in the absence of appropriate juridical or parliamentary oversight which in turn has propelled a worldwide discussion of individual right to privacy as well as the means for the state to maintain security and go about the surveillance process.

b) **United Kingdom- Investigative Powers Act:** On many occasions this tracking is criticized for its scope and the UK Investigative Powers Act allows the surveillance of telecommunications data in bulk. There is an opinion that this is an illustration of the excess of authority, due to the mass surveillance of citizens without any control or clear links that the security should have while carrying out investigations.

4. Article 19(1)(a) and Freedom of Expression

[8]U. Sarkar, M. Saleem & K. Sanjaya, Right to freedom during COVID-19: a study of Article 19 of the Indian Constitution in light of COVID-19, 1 Int'l J. Pub. L. &Pol'y 1 (2023).

4.1 Constitutional Provisions

Article 19(1)(a) of the Indian Constitution is the cornerstone of the structure of democratic rights given to the citizens of India, ensuring that freedom of speech and expression is granted. This covenant has generically two-dimensional meaning first personal freedom of person as well for the healthy work of democracy avoiding any connections, criticizing government actions, and exchange of ideas without fear of oppression[8].

Text and Interpretation of Article 19(1)(a)

It 19(1)(a) says that every citizen should have the right to speak out and be heard. This right is vast and has been interpreted to encompass the liberty to express one's views through any means of communication, like words (spoken or written), pictures, films, or any other communication channel. It is embodied in everything starting from the paper publication of newspapers, magazines and books up to broadcasting in radios or televisions and extends to more modern means of expression such as the Internet and social networks.

Scope

While the freedom of speech is a very important right, it needs to be considered in a context as it is not absolute either. Article 19(2) of the Constitution is the provision which specifies the grounds on which the state can impose the reasonable restrictions on this right. The said grounds involved the supremacy and integrity of India, the state's security, cordial relation with other countries, public order, decency, or morality, and in relation to contempt of court, defamation, or incitement to an offence. The case is that individual freedom be restricted only once it would be against the common good.

The Supreme Court of India has enjoyed a moment in history where it was responsible for setting the parameters of 'reasonable restrictions'[8]. The Superior Court has always been saying

[8]M. Susi, Human Rights, Digital Society and the Law (May 31, 2019).

[8]A. Keer, Digital Transformation in Government Procurement: Assessing the Impact of GeM in India, 12 Int'l J. Sci. & Res. (IJSR) 2010 (Nov. 5, 2023).

that any restriction must be a reasonable and essential one in a democratic society. Discussion on the scope must not also be wide and vague but must be shorter and go straight toward the objectives stated in Article 19(2). It must also not cut the essence of freedom granted under Article 19(1)(a).

Judicial Interpretations and Landmark Judgments

Since its enactment, a number of significant verdicts have unravelled what is regarded as Article 19(1)(a). The Thappar vs Madras State case (1950) the Supreme Court decided that the issue of freedom of speech and expression was essential in order for the country's constitution to be valid, meaning that a law which restricts these rights could only be supported if there was a real need to do so. Secondly, in Sakal Papers v. Union of India (1962), the Court ruled against the governments' try to regulate the price and number of pages in newspapers and anticipated it as one of the infringement to Article 19(1)(a).

Modern Challenges and Digital Realm

In the digital age, the use of Article 19(1)(a) has expanded to include internet and mobile communications, which the Supreme Court has reaffirmed as part of the right to freedom of speech and expression in the Shreya Singhal vs. Union of India (2015). This case has further revealed that section 66A of the IT Act which inhibits the Internet users through unclear wordings of the law is unconstitutional[8].

4.2 Judicial Interpretations

The right to free speech and expression guaranteed under Article 19 (1) (a) of the Indian Constitution has endured a lot of judicial interpretation due to various reasons. Over the years, the Supreme Court of India has made many decisions that have a great impact on the meaning and the application of this fundamental right, drawing the line between its scope and limitations.

Landmark Judgments

[8]A. Paunksnis, India digitalized: surveillance, platformization, and digital labor in India, 24 Inter-Asia Cultural Stud. 297 (Apr. 3, 2023).

i. **Romesh Thapar vs. State of Madras (1950):** Inspired by this first case, this principle is also reflected in the later cases that formed the body of free speech jurisprudence in India. The Supreme Court declared invalid the Madras government decision which prohibited a communist newspaper from entering and circulating within the state. The freedom of speech and expression could only be restricted if the restriction was of the same kind as those that were allowed under Article 19(2) and this restriction could reach only the ends that Article 19(2) permits[8].

ii. **Brij Bhushan and others vs. The State of Delhi (1950):** The very next case after their landmark RomeshThappar case was the Supreme Court considering the question of pre-censorship of English weekly in Delhi. The Court held that the practice of press pre-censorship was an abridgement of the freedom of press unless it was clearly shown to be necessary to prevent an imminent catastrophe or the existence of substantial danger to the society.

iii. **Sakal Papers (P) Ltd. vs. Union of India (1962):** The government in a manner to control the financial issues of a newspaper might have genuinely meant to stamp out the unfair competition. The daily newspaper was freed from the necessity to conform to the Price and Page Act, 1956, as the Supreme Court ruled that it amounted to a direct interference with the press. The Court clearly demonstrated that any restriction on the flow, publication, or the price of newspapers would directly curtail the freedom of expression.

iv. **Kedar Nath Singh vs. State of Bihar (1962):** The present dispute deals with the legitimacy of some articles of the code that punishes pamphlets which can provoke crimes against the state as prescribed under the Indian Penal Code. The Supreme Court gave permission to this legislation and narrowed its scope by interpreting its provision, so that they would now only refer to acts involving such intention or tendency to create disorder, or disturbance of peace and calm or incitement to violence.

v. **Shreya Singhal vs. Union of India (2015):** As the case of Shreya Singhal, Supreme Court ruled down Section 66A which was a part of the Information Technology (IT) Act, 2000, that considered sending offensive messages through communication services

[8]R. Ó Fathaigh, J. Möller& R. Bellanova, DIGITAL PLATFORMS AND THE DIGITISATION OF GOVERNMENT SURVEILLANCE, AoIR Selected Papers Internet Res. (Sept. 15, 2021).

illegal. This part of the law was found to be unconstitutional because it was not specific enough and it was too broad and can potentially be used to criminalize a lot of speech that should be protected under Article 19(1)(a). The case law provided a sensitive look into the protection of speech in the modern era requiring legislation that determines clear and present danger and limits justifiable interference to speech[8].

4.3 Conflict and Surveillance

The government surveillance sometimes regrettably go to the extent where it tampers with both the national security and the freedom rights especially the privacy and free speech. In certain places around the world, such as India, the delicate balance between prosecutors and constitutional rights has been disturbed on several occasions, resulting in serious clashes with constitutional rights. The biggest struggle in India probably came out with the revelations of the CMS and the NETRA systems[8]. Those programs mainly served to bolster the mechanism of intercepting and monitoring communications and internet streaming. Nevertheless, they were seriously concerned about the privacy problems as a result of the lack of transparency and accountability in their operations. It was argued that straightforwardly deployed surveillance power would be in contradiction to the so called 'Right to Privacy' for which the Indian Supreme Court had suggested in the Article 21. Supreme Court's remarkable verdict by the name of Justice K. S Puttaswamy (Retd.) vs. Union of India aired in 2017 has been acclaimed as the landmark moment in the history of the individual's right to privacy. The Union of India (2017) stressed on privacy as a basic right and thus, any interference in privacy by the state actions must be justified through a law that is reasonable and proportional to the situation.

The constitutional validity debate of the Aadhaar project also shows the friction between government surveillance and constitutional rights. The Jan Dhan scheme that was introduced for creating a novel biometric database for everyone was taken on the pretext that it might lead to widespread surveillance. The Supreme Court gave its verdict that Aadhaar was within the Constitution but ruled out certain provisions from the surveillance state that could have resulted

[8]P. N. Thomas, The Politics of Digital India (July 11, 2019).

[8]R. A. Cropf, Ethical Issues and Citizen Rights in the Era of Digital Government Surveillance (Feb. 2, 2016).

of linking Aadhaar to bank accounts or phones without proper provisions in law. Internationally, the Edward Snowden revelations in 2013 uncovered the amount of electronic surveillance by the US National Security Agency (NSA) and this has triggered worldwide discussions on the right to privacy and freedom of speech. The got-out-of-hand documents having revealed NSA's activities regarding massive gathering of phone and internet data, not only from Americans but also from foreign nationals without legally acceptable and public oversight. This issue caused worries about how much power the government has to count as intrusion and was followed by a public outcry and calls for the reform of such surveillance which underlined the tension between the national security interest and the constitutional rights that the citizens are meant to enjoy. . Such cases highlight the constant conflict between the government's responsibility to safeguard its people and the obligation to respect and uphold the Constitution. Every scenario becomes an analytical compass of how the world in general, and nations in particular, confront with the intricate set of relationships between security and freedom, which is above all subject to the development of technology that influences those contours.

5. Balancing Act: Surveillance for Security and Protecting Rights

5.1 Necessity of Surveillance in National Security

The role of national and societal security and order cannot be overestimated with modern technology posing a variety of threats that not only sophisticated but also unpredictable. Surveillance has a significant role to play in governments' efforts to detect and respond to incidents such as terrorism and organized crime, cyber threats and espionage. This mechanism of conflict prevention is not only necessary for the establishment of safety and tranquillity of the state itself, but also for its citizens.

Data collection and its analysis is made possible by surveillance which as a white collar universally accepted norm are important as a preventive measure in terrorism. After the 9/11, the majority of the countries enhanced their surveillance systems to detect and disrupt the terrorist plots before they turn into a reality. As an instance, security agencies' capabilities expanded to include monitoring communications so that they can identify and follow terrorist cells, which may be planning terrorist attacks. The preventive role of this approach is of course without a

doubt, and its importance is ever the more critical in an environment where there are still myriad terrorist challenges. Also, surveillance is a must in dealing with the organized crime such as drug trafficking, human trafficking, and arms smuggling. Effects of surveillance networks and employing the use of technologies such as CCTV and satellite imagery may break up networks of criminals working across state lines. Besides being a significant weapon by the police to prevent and arrest criminals, these highly tractable systems elicit more intelligence that in turn serve as further clues to perpetrators' hideout and future planning.

The emergence of cyber threats has also made the surveillance more vital. In the current situation, when cyber attacks can lead to shutdown the infrastructure, data leakages, and even election influences, governments need to build effective mechanisms to fight against these problems[8]. In cyber domain, monitoring is one of the most important duties; preventing, and where possible, detecting unusual online activities, and intercepting the traffic that would signal malicious intent against national critical infrastructure. On top of that, surveillance is a major factor in the provision of public safety through the improvement of the responsiveness of the emergency services. Shown top is an instance when surveillance gadgets can offer instant information which is fundamental in coordinating immediate and effective responses during instances of natural disasters or major accidents. For instance, drone surveillance can deliver this type of information in a quick way.

5.2 The Right to Privacy and Legal Limitations

The most important judicial confirmation of privacy as a fundamental right came with the Supreme Court's unanimous decision in Justice Puttaswamy (Retd.) vs. Union of India (2017). Up in this case the Court has said that right to privacy envelops into the larger constitutional freedom which originates mostly under Article 21 which is the right to life and personal liberty

[8]Irshad, E., & A. Basit Siddiqui, Cyber threat attribution using unstructured reports in cyber threat intelligence, 24 Egyptian Informatics J. 43 (Mar. 2023).

in the Constitution. The court recognized privacy, which in the present day, where technology has become of great concern is an important issue. The Court not only identified privacy as an inalienable part of life and personal liberty but also laid down that any intrusion into privacy by the state has to satisfy the three-fold requirement of legality, which includes the existence of a law; legitimacy, meaning it must serve a legitimate state purpose; and proportionality, which ensures that the means used are strictly necessary for the achievement of the objective[8].

This decision etches out an important milestone in the safeguarding of our privacy from intrusive electronic surveillance methods. The state is, in many cases, legitimized in the use of surveillance by using such arguments as safeguarding national security, guaranteeing order in the public space, and curtailing objectionable behaviour. Some of these reasons are acceptable under article 19(2) which allows justifiable restrictions on fundamental rights. Nevertheless, the scope and the amount of these surveillance activities are sometimes a matter of contention as they are seen as a violation of the right to privacy. For example, if mass surveillance programs are not checked and are not clear about their aim of the information they gather, an extreme invasion of privacy could happen, which would violate the proportionality which ensured by the Supreme Court. The issue of balancing the right to privacy and the state surveillance becomes more apparent as well in the discussions dedicated to the legal aspect and the ethics of projects such as Aadhaar and other mobile application-based tracking formulated as the public health or the safety measures, and particularly noticeable during the pandemic caused by the COVID-19 virus. These systems, which are designed to gather a lot of personal information, have been criticized for the lack of robust privacy protections and the potential misuse of data.

As far as the surveillance operation program is concerned, without the voluntary tacit state surveillance system and comprehensive oversight, independent judicial pre-approval or review must be provided. Thus, it will guarantee that surveillance measures are not only lawfully sanctioned but also in compliance with the principles of necessity and proportionality, in order to avoid arbitrary and excessive government intrusions into individuals' private lives.

5.3 International Perspectives and Best Practices

[8]C. Arun, Gatekeeper Liability and Article 19(1)(A) of the Constitution of India, SSRN Electronic J. (2015).

Of the delicate balance between state surveillance, personal freedom and the free exchange of ideas, finding an appropriate global solution, with every government taking different measures to safeguard these complex issues, is one of the toughest challenges. This study finds out several important international legal regulations, viz., the General Data Protection Regulation of the EU, the USA PATRIOT Act and it compares them to practices elsewhere[8].

European Union: General Data Protection Regulation (GDPR)

The GDPR that was brought into effect in May 2018 is one of the most stringent and comprehensive data protection laws in the world. The main objective was to develop rules that would safeguard the personal data of individuals in the European Union to reflect changes in the rapidly developing technology. The essential elements of the GDPR, in which transparency, provision of security, and accountability of personal data processors, along with confidentiality of information, are considered primary, while giving people a right to control their personal information even more compared to before the GDPR. This principle is not limited to the firms located in the EU, but it also applies to those who are managing data of EU citizens from outside the EU.

This regulation also deals with the issue of consent acquisition which has to be a clear, distinct, full and accurate. That helps to reinforce the individual's right for the privacy and autonomy of the data being collected and processed, thus requiring that the data collection and processing were not merely legal but also just and transparent. Furthermore, the GDPR specifies very tough rules in respect of the data transfer to non-EU countries, thereby guaranteeing that the level of privacy protection is not reduced. The regulation, thanks to fines at a significant level, becomes a potent tool to enforcement of personal data standards by developers and companies.

USA: USA PATRIOT Act

On the contrary, the USA PATRIOT Act, passed in the wake of the September 11 attacks in 2001, was very different from the GDPR. This law greatly enhanced the powers of the American law enforcement for the declared purpose of fighting terrorism. Besides the Act

[8]Daniel J. Solove, the Digital Person (2022).

expanded the range of surveillance the scope which includes wire tapping, communication interception, and getting hold of business records. This legislation however comes up with these provisions of oversight, which include the need for permission from the Foreign Intelligence Surveillance Court (FISC)[8]. Thus the critics argue that this expansion is very wide and somehow very intrusive.

The USA PATRIOT Act has been criticized for the possibility of a breach of privacy rights and restriction of the freedom of expression by creating a culture where people might feel under surveillance and thus, less free to express themselves. This Act reveals a law which is harsher in nature and, where the proportion is more tilted to empowering law enforcement and intelligence agencies, individual's rights are less cared about.

Comparative Reflection

An eminent disagreement within the principles that the Europe GDPR & the USA PATRIOCT Act comprise is evident. The GDPR is designed to safeguard the rights and privacy of individuals, requiring strict accountability and openness in data processing. While America Patriot Act (Patriot Act) focuses on improving national security framework, some liberties especially the ones on personal privacy and liberty of expression may be put aside at times.

This conflict exemplifies the clash in legal schools of thought and priorities in the EU and the US—privacy and freedom of choice on one side and an unbridled governmental power on the other. Every method has its strengths and weaknesses and the biggest challenge for all democratic countries is to find a legally and morally acceptable way to balance security and liberty. The relationship between the EU and the US also involves the issue of the conflicting approach in the way both sides interpret the significance and implementation of privacy rights and which significantly affects issues such as free data exchange and international law enforcement cooperation and counter-terrorism.

6. Regulatory Frameworks and Reforms

[8]Donohue, L. K., Surveillance, State Secrets, and the Future of Constitutional Rights, 2022 Sup. Ct. Rev. 351 (June 1, 2023).

6.1 Existing Legal Safeguards and Their Efficacy

Fairness and privacy of the individual are the crucial goal of legal frameworks in many countries that allow or stand against states' communication control. Such regulations often engender the list of limitations on the application of powers of surveillance, legalization of such process and controls over it as well as the accountability. Nevertheless, the efficiency of these legal guarantees is not the same, and usually it is determined by the political and legal background of the country.

Such vetting procedures are aimed at making sure to prevent any infringement on the balance between state security and personal rights by democracies. To clarify take the instance in the United States's FISA was established to warrant the approval of the FISA Court for the surveillance stemming from foreign intelligence purposes. In the same way, the Indian Telegraph Act and the Information Technology Act provide the mechanisms for surveillance like the need for government authorization and oversight. Nevertheless, the question arises as to how efficient precisely these safety measures are. Some critics believe that the processes could be rather trivialized and mysterious, with no necessary transparency of the decision-making algorithms regarding surveillance authorization and lack of sufficient redress mechanisms for the individuals targeted by surveillance. The main problems of the effectiveness of these safeguards lie in the fast development of technology that is ahead of the legal developments, the broad and sometimes vague language of statutory authorizations, and the limited capacity of oversight bodies to effectively monitor and enforce compliance with the law.

6.2Proposed Legal Reforms

To address these challenges and improve the balance between surveillance and civil liberties, several legal reforms can be proposed:

a) **Enhance Transparency and Oversight:** Making the surveillance process more transparent and the decisions are available to the public can be an exercise of strengthening the public trust and accountability. Consequently, the agency agencies shall be obliged to keep records of their surveillance and issuing regular reports about how much of it has been performed and in what regard, as well as the re-organization of the legislative oversight committees.
b) **Strengthen Judicial Review:** Rendering the judiciary empowered to issue surveillance authorizations further grant a more balanced power contrast. This can include the judicial review for not only the legality but also the necessity and proportionality of the surveillance measures that are being proposed.
c) **Update Legal Standards:** Since technology keeps on developing, it is upon the law makers to review the legal standards on surveillance often, from time to time in order to remain relevant. Legislatures must work hard on rewriting monitoring laws which take facial recognition as well as AI based data analysis into account so that such technologies are not used for reasons that violate individuals' privacy rights.
d) **Protect Against International Overreach:** In the wake of the growing flow of data across borders, domestic legislations should also take into account the international aspect of surveillance. It entails the tightening of spying safeguards against disclosure to external entities and the reinforcement of legal mechanisms and partnerships in law enforcement and intelligence that respect human rights and individual liberty.

6.3 Role of Judiciary and Independent Bodies

Governments targeted judiciary and independent regulatory bodies to take charge of the surveillance issues within the government. Their ability to perform their duties properly is mainly determined by their independence, authority, and the resources they have at their disposal.

a) **Judiciary:** Judicial authorities always have a power to examine the government's needs for surveillance and thus act as a legal balancing feature that determines under what circumstances and in what way a surveillance is done. Even in the U. S., FISA Court makes warrant application for surveillance intruding on national security. The judiciary's

ability to carry out this function might be weakened by the absence of technical knowledge and by the often secretive character of national security information, which limits the courts to assess the justification for the surveillance measures in full.

b) **Independent Bodies:** The surveillance of governments should be done by independent and transparent bodies like position commissioners, a surveillance watchdog, etc. The bodies apart from examining complaints and analyzing the surveillance policy of the government can also offer recommendations on proposed changes. The ability of their effectiveness is intensified when they have the necessary legal powers, resources, and genuine independence from the government[8].

7. Conclusion

Summary of Key Findings

This research uses a comprehensive approach to identify the subtle equilibrium between government spying and the protection of constitutionally guaranteed freedoms, particularly freedom of expression as stated in Article 19(1)(a) of the Indian Constitution. Surveillance, first and foremost, it is justified through the lens of the country' individual safety and public control, nowadays, it is almost attached by technology especially with the advancement of surveillance tools, which in turn raise major privacy and free speech concerns. This research draws attention to the threat of a state's excessive power purported by encroachment on digital rights, therefore underlining the need for a legal basis that guarantees the rule of law and its three main foundations, that are; necessity, legality, and proportionality.

Future Outlook

In the future, law enforcement surveillance is going to be changing, and this will be to a large extent led by the rapid advances in the fields of artificial intelligence, data analytics and

[8]P. K. Jha, A. T. Polcumpally& V. Saigal, Emerging Digital Technologies and India's Security Sector (June 7, 2024).

biometric technologies. This growth in capabilities demands to capture up the legislation and monitoring institutions so that they are ready for the new challenges and are no longer afraid to use their power against privacy and surveillance. Also, as information exchanges are undertaken through a growing number of digital platforms on a worldwide level, international cooperation and uniformity of surveillance legal rules will turn out to be very significant. Also, the future developments should include the upgrading of the importance of judicial oversight and the enhancement of independent regulatory bodies to prevent the violation of constitutional rights.

Final Thoughts

Finding a balance that deals with the security needs and the fundamental rights deserves a special attention; otherwise, it will be difficult to achieve security in an open and pluralistic society. The indisputable necessity of surveillance for protecting national security and public safety is not to the same extent permissible for being a violation to the democratic values the surveillance itself is supposed to ensure. This is not a balancing act that is once and for all but a process that is under constant reassessment to cope with the new challenges and technologies. Secrecy in surveillance operations is worth a crack as a universal principle. It should be complemented by transparency, enhancing judicial and independent oversight mechanisms, and stimulating public dialogue on this topic. Through ensuring that people are protected by rights that are the foundation of any democratic community, we will at the same time be able to effectively tackle the wide range of security difficulties seen in the contemporary world.

8. References

1. Kashyap, Importance of Freedom of Press under the Ambit of Article 19(1) (A) of the Indian Constitution, 12 Int'l J. Sci. & Res. (IJSR) 1538 (Nov. 5, 2023).
2. B. Pandey, Review Article- The Supreme Court and the Constitution: An Indian Discourse, SSRN Electronic J. (2020).
3. U. Sarkar, M. Saleem & K. Sanjaya, Right to freedom during COVID-19: a study of Article 19 of the Indian Constitution in light of COVID-19, 1 Int'l J. Pub. L. &Pol'y 1 (2023).
4. R. Kohli, Expressive Conduct and Article 19(1)(a) of the Indian Constitution: A Purposivist Approach, 16 Asian J. Comp. L. 259 (Oct. 12, 2021).
5. C. Arun, Gatekeeper Liability and Article 19(1)(A) of the Constitution of India, SSRN Electronic J. (2015).
6. J. Subhan, Emerging Rights Under Article 19(1)(a) of the Constitution of India, SSRN Electronic J. (2010).
7. S. Coliver& A. 19, The Article 19 Freedom of Expression Handbook (Jan. 1, 1993).
8. G. Bhatia, Offend, Shock, or Disturb (Jan. 14, 2016).
9. D. Cole, Secrecy, National Security and the Vindication of Constitutional Law (Jan. 1, 2013).
10. M. Susi, Human Rights, Digital Society and the Law (May 31, 2019).
11. G. Goyal & R. Kumar, The Right to Privacy in India (Jan. 11, 2016).
12. V. D. Mahajan, The Constitution of India (1963).
13. A. Keer, Digital Transformation in Government Procurement: Assessing the Impact of GeM in India, 12 Int'l J. Sci. & Res. (IJSR) 2010 (Nov. 5, 2023).
14. A. Paunksnis, India digitalized: surveillance, platformization, and digital labor in India, 24 Inter-Asia Cultural Stud. 297 (Apr. 3, 2023).
15. R. Ó Fathaigh, J. Möller& R. Bellanova, DIGITAL PLATFORMS AND THE DIGITISATION OF GOVERNMENT SURVEILLANCE, AoIR Selected Papers Internet Res. (Sept. 15, 2021).
16. V. R. Rao, A framework for unified digital government: A case of India, 36 J. E-Gov. 35 (2013).
17. P. N. Thomas, The Politics of Digital India (July 11, 2019).
18. R. A. Cropf, Ethical Issues and Citizen Rights in the Era of Digital Government Surveillance (Feb. 2, 2016).
19. Donohue, L. K., Surveillance, State Secrets, and the Future of Constitutional Rights, 2022 Sup. Ct. Rev. 351 (June 1, 2023).
20. P. K. Jha, A. T. Polcumpally& V. Saigal, Emerging Digital Technologies and India's Security Sector (June 7, 2024).
21. M. K. Deep, Digital India Mission. Implications on Social Inclusion and Digital Citizenship (Mar. 5, 2018).
22. Daniel J. Solove, The Digital Person (2022).
23. P. Manning, The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement, 48 Contemp. Soc. 170 (2019).
24. J. Mandelblatt et al., Collaborative Modeling of the Benefits and Harms Associated With Different U.S. Breast Cancer Screening Strategies, 164 Annals Internal Med. 215 (2016).
25. Irshad, E., & A. Basit Siddiqui, Cyber threat attribution using unstructured reports in cyber threat intelligence, 24 Egyptian Informatics J. 43 (Mar. 2023).