
GOVERNMENT SURVEILLANCE & THE RIGHT TO PRIVACY: A COMPARATIVE CONSTITUTIONAL ANALYSIS OF INDIA, THE EU & SWITZERLAND

Mr. Hetkumar Joshi¹, LL.M. (Intellectual Property),
Amity University, Noida, Uttar Pradesh, India.

ABSTRACT

“Privacy is a basic human right, not a privilege”. In India, after the landmark judgment of *K.S. Puttaswamy v. Union of India*² the Right to Privacy was established as a sword cast upon the State to protect the privacy of all persons and, at the same time, to shield them from unwarranted intervention by the State in the privacy of individuals. The State has undergone a digital transformation, and the governance of individuals is now data-driven. The State has been collecting information about individuals through multiple platforms as part of mass surveillance systems, collecting various types of data. The collection of such a large number of people in India has raised questions regarding the encroachment upon the private lives of individuals by the State and the further infringement of informational autonomy.

In such circumstances, the privacy of individuals becomes vulnerable, as accountability for such infringement and the indiscriminate collection of data under the pretext of State security shall be subject to judicial adjudication and scrutiny. The paper analyses the existing developments in State-led digital surveillance of individuals and the legal framework compelling the State to adhere to privacy standards, with a comparative study of the European Union’s “Rights-First” model and Switzerland’s “three-layer shield” for the protection of privacy and other laws of the respective States.

Keywords: Right to Privacy, State Surveillance, Data Collection, Data Protection, Digital Governance.

¹ LL.M. (Intellectual Property), Amity University, Noida, Uttar Pradesh, India.

² Justice K.S. Puttaswamy (Retd.) v. Union of India, AIR 2017 SC 4161.

I. INTRODUCTION

1.1 Background and Evolution of Right to Privacy

The Right to Privacy was first defined as the “*Right to be let alone*” by Samuel D. Warren and Louis D. Brandeis in the article titled “*The Right to Privacy*”, which was published in the Harvard Law Review³. The philosophical idea behind the article, which evolved, was to establish a separate legal principle to protect the dignity of the individual with significant changes in the world. Post World War II, the first global recognition of the Right to Privacy was established by the United Nations under Article 21 of the Universal Declaration of Human Rights, 1948 (UDHR) that states that “*No one shall be subjected to arbitrary interference with their privacy, family, home or correspondence, nor to attacks upon his honour and reputation*”⁴.

Subsequently, the first Judicial approach amongst all judicial systems that recognised the Right to Privacy as a fundamental right was held by the U.S. Supreme Court in the year 1965, wherein the Court ruled that the “zone of privacy” is protected from State regulations and established the doctrine of “*decisional privacy*”⁵. Further, the USA expanded the decision again in the year 1973 and held that decisional privacy is protected under the concept of personal liberty⁶. Further, the evolution of the Right to Privacy was adopted in legislation, and nationwide laws were implemented, such as the Sub-National Data Law in Germany⁷. In the year 1970, the *Datalagen Act* of Sweden was enacted in 1973⁸ and thereafter the US Privacy Act in 1974⁹. All of the developments of globally recognising the Right to Privacy through different organs further divided the right into two parts, i.e. a) Decisional privacy and b) Informational privacy, which raised concepts such as data control, digital security, information consent and State non-interference.

In India, the Right to Privacy has never been expressly written as a Fundamental Right in the Constitution. The emergence of the Right to Privacy in India is largely dependent on the judicial interpretations of Article 21 of the Constitution. Article 21 of the Indian Constitution assures

³ Samuel D. Warren, Louis D. Brandeis, *The Right to Privacy*, Harvard Law Review, Vol. 4, No. 5 (1890).

⁴ India Const. art. 21.

⁵ *Griswold v. Connecticut*, 381 U.S. 479.

⁶ *Roe v. Wade*, 410, U.S. 113.

⁷ *Datenschutzgesetz* (Data Protection Law), GVBl. I 625 (Hesse 1970) (Ger.).

⁸ *Datalag* (Data Act), SFS 1973:289 (Seed.).

⁹ *Privacy Act of 1974*, 5 U.S.C. section 552a (1974).

that “No person shall be deprived of his life or personal liberty except according to procedure established by law¹⁰”, while the judiciary, by purposive interpretation, held that the assurance of the right to life and liberty under Article 21 would become meaningless without protecting privacy¹¹. However, the Right to privacy in India was earlier interpreted by the Supreme Court as a right which is not identified as a fundamental right in the Indian Constitution, unlike the US’s Fourth Amendment¹² and a right that is not guaranteed by the Constitution¹³. Simultaneously, transformative constitutionalism took place and the judicial shifts rejected the hard words of past rulings and a landmark judgment in *K.S. Puttuswamy* was ruled declaring that Privacy as an essential part of dignity, autonomy and liberty of individuals inherited under Article 21 and further held the Right to privacy as fundamental and inalienable right¹⁴.

1.2 Privacy in the Age of Surveillance

In the Digital era, every other area is being technologically advanced, and every other activity on any network is being watched. Every click of an individual has been recorded in the form of data, which is later used by tech giants and governments for surveillance and economies¹⁵. With growing digitalisation, the government has enrolled the surveillance of individuals based on digital Biometric Systems, Facial Recognition Technology, communication interruption, AI-Driven surveillance and other major mass surveillance systems. Under the mass grid of constant monitoring by the government, the privacy of individuals has become vulnerable. As the price of constantly being watched on digital platforms has raised the question of whether data collection by the Government has been used for protection or is being used as a medium to control, and whether the privacy of the individual is being respected with the rules and regulations laid down by the precedents.

After the rulings by the Supreme Court, the factor of data surveillance by the State remains unchanged. Such, mass surveillance by State agencies leads to the question of the areas such as State accountability, loopholes in legislation and exemptions of State authority, and the independent intervention of the judiciary is still a drawback and a serious issue threatening the Right to Privacy of individuals. The gap between the Judicial rulings considering privacy as

¹⁰ India Const. art. 21.

¹¹ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, AIR 2017 SC 4161.

¹² *M. P. Sharma v. Satish Chandra*, 1954 SCR 1077.

¹³ *Kharak Singh V. State of U.P.*, AIR 1963 SC 1295.

¹⁴ India Const. art. 21.

¹⁵ “Digital Surveillance Laws in India”, *Lloyd Law College*, <https://www.lloydlawcollege.edu.in/blog/digitalsurveillance-laws-india.html>.

inherit right of the Constitution and the ground-level reality remains unvaried.

II. GOVERNMENT DATA SURVEILLANCE AND ITS IMPACT ON THE RIGHT TO PRIVACY

2.1 Government Initiatives and Technological Developments Facilitating Data Collection

2.1.1. Aadhaar and State-Based Identity Infrastructure:

One of the most prominent programmes introduced by the government to record the data of the individual was the Aadhaar system that was introduced on 28th January, 2026 by the Unique Identification Authority of India (UIDAI) for the purpose of universal identity, transparent welfare delivery, and other purposes. The UIDAI, through the Central Identities Data Repository (CIDR) collected the “Know Your Resident” (KYR) data, which includes the Demographic Data that are Name, date of birth, gender and address and Biometric Data that includes 10 fingerprints, 2 iris scans, and a facial photograph for making the database of each individual having a unique Aadhaar number¹⁶. This type of Data collected by the government is termed as “Context-Independent Data” because such type of data is only for the purpose of verification of identity and does not collect the socio-economic data of the individuals¹⁷. Aadhaar became a pioneer for subsequent data collection programs introduced by the government.

To further govern the operation of Aadhaar, the government implemented the Aadhaar Act, 2016. However, Aadhaar faced constitutional challenges in the landmark judgment of *K.S. Puttaswamy vs Union of India (2017)*, where the Supreme Court, after scrutiny, established the Right to Privacy as the fundamental right and ruled the “triple test” principle that the State must follow to collect the Data of the individual. The triple test that shall be followed by the State includes (i) legislative backing, (ii) a need of law, and (iii) proportionality for implementation of such programs that put the privacy of individuals at risk.

The rulings are strictly applicable, but despite this, a shift was observed by the researchers. The researcher highlighted that the collection of “Know Your Resident” (KYR) data of individuals was aggregated with the State welfare database and is forming the State Resident Data Hubs

¹⁶ Unique Identification Authority of India, *Features of Aadhaar*, <https://uidai.gov.in/hi/features-of-aadhaar>

¹⁷ Chaudhuri, B., & Subrahmanian, *Privacy and Security of Aadhaar: A Computer Science Perspective*, (Indian Institute of Technology Delhi (IITD) Technical Report 2015).

(SRDH). This linkage of the Aadhaar authentication numbers and the “Know Your Resident” (KYR) Data of the individual resulted in the generation of another type of Data that is “Context-Dependent Data”.

The interconnectivity of the context-independent and the context-dependent data of the individuals made a bridge between the data used for the identification of the individual with activities and status that an individual has performed and may hold, resulting in an inescapable loop of private life being watched by the government. These linkages open the window for the government to monitor the behaviour of individuals across all the sectors, such as the caste of the individuals, land transfer and purchase, utility consumption, and others that are interconnected via a common database holder that is the government¹⁸.

This is the point where the privacy of individuals gets affected, as one single activity of the individuals has to be reflected across all the sectors of the State holdings. The State, by creating the “360-degree database” of the individuals, cleverly surpassed the strict implementation for the protection of privacy and created a siloed protection that results in a “single source of truth” revealing the whole private life of an individual¹⁹. These interconnected mechanisms help the State to form a profile of the individual’s life cycle, including birth, marriage, migration, socio-economic condition and others without their implied consent²⁰. The said “State-facilitated profiling” of an individual creates a mass surveillance mechanism that can be utilised by the State at its own will to infringe the privacy of individuals without any adherence to strict rulings²¹.

The Aadhaar data system has weaknesses in the process of authenticity and a direct impact on the privacy of individuals by constantly monitoring the activity of the individuals. By technically analysing the Aadhaar ecosystem, the loophole leading to infringement of privacy is identified. Every identification process at any agency of an individual where Aadhaar authentication is used, be it a hospital, bank or etc., creates a “metadata trail” or “authentication log”²². This metadata or log, which is collected from the agencies, records the location, time and details of agencies where the individual’s Aadhaar authentication is being recorded.

¹⁸ Venkatanarayanan, A. *The 360 Degree Database: Understanding State Resident Data Hubs*, Medium (2017).

¹⁹ Venkatanarayanan, A. *The 360 Degree Database: Understanding State Resident Data Hubs*, Medium (2017).

²⁰ *The Threat of Aadhaar-Enabled Surveillance*. Swarajya Magazine (Technical Policy Review).

²¹ Reetika Khera, *Dissent on Aadhaar: Big Data Meets Big Brother* (Orient BlackSwan 2019).

²² Chaudhuri, B., & Subrahmanian, (2015). *Privacy and Security of Aadhaar: A Computer Science Perspective* (2015).

Thereby, when all this data of individuals is aggregated forms “real-time tracking” data of individuals, locating the individual’s activities, patterns, behaviour, movements, habits and all other activities that an individual does in the life cycle²³. This constant tracking by the government leads to the violation of the right to privacy of individuals, as such monitoring is not consented.

2.1.2. Government Platforms and Interconnected Data Systems:

The government in the past few years has generated a 360-degree profile of individuals by monitoring and tracking all the activities, including biometric, telecommunications, financial condition, travel, and many others. The automated surveillance of the individual’s daily lifestyle is interconnected through certain government platforms dedicated to different fields. The following are different platforms by the government:

(i) National Intelligence Grid (NATGRID):

The National Intelligence Grid (NATGRID) is an integrated intelligence platform operated by the Ministry of Home Affairs. The NATGRID collects data from 21 separate categories, including bank transactions, financial logs, immigration logs, income tax returns, card logs, telecommunication logs, vehicle registrations, and others²⁴. The NATGRID works on a secure federated query system rather than a single centralised database²⁵. The system processes data via dedicated hubs and collects the sovereign databases via independent third-party providers²⁶.

(ii) Crime and Criminal Tracking Network (CCTNS):

The Crime and Criminal Tracking Network & Systems links 14,000 police stations across India, making a single network for all the First Information Reports that are being filed and the criminal records²⁷. This collection of all the FIRs and criminal

²³ Bhatia, A., & Bhabha, J. (2017), *India’s Aadhaar Scheme and the Promise of Inclusive Social Protection*, Oxford Development Studies, (2017).

²⁴ Model Diplomat, *NATGRID*, <https://modeldiplomat.com/learn/glossary/natgrid>.

²⁵ Press Information Bureau (PIB), Government of India, *Ministry of Home Affairs Status Report on NATGRID (2022)*, <https://pib.gov.in>.

²⁶ A. Kumar, A., & Singh, R., National Intelligence Grid (NATGRID): An Overview and Comparative Analysis of Global Counter-Terrorism Legislation, 12(3) International Journal of Legal Studies.

²⁷ Ministry of Home Affairs. (n.d.). Crime and Criminal Tracking Network & Systems (CCTNS) Portal. Government of India. <https://mha.gov.in>.

records is being synchronised to the National Data Centre (NDC), which comes under the National Crime Records Bureau (NCRB)²⁸. The Data that is collected and stored are the arrest histories, fingerprints and general police station diaries.

(iii) Central Monitoring System (CMS):

The CMS collects the data of live mobile calls, messages, metadata and real-time internet usage²⁹. Such private data is directly collected by Telecom Service Providers (TSPs) and Internet Service Providers, bypassing the involvement of the service provider directly from the Regional Monitoring Centres (RMCs)³⁰. The system, without any notification or specific reasoning to the individual, allows the State to record all the conversations without any limitations.

(iv) Automated Facial Recognition System (AFRS):

The AFRS is administered under the NCRB. The AFRS collects data of digital facial images, biometrics and video feeds from CCTV feeds and public repositories and converts them into mathematical templates that are searchable³¹. The system works without any legislative oversight and escalating risks of function creep³².

(v) Network Traffic Analysis (NETRA):

The NETRA is developed by the DRDO. The NETRA works on the major internet gateways and routers and thereby filters the raw data³³. The system intercepts the data traffic, web logs, emails, instant messaging and other types of data available. The filtered data is stored in conversational segments across the intelligence agency servers

²⁸ Narayan, S. (2017). Smart Policing, CCTNS, and the Right to Privacy in India. *Economic & Political Weekly*, 52(14), 22-25.

²⁹ Rajya Sabha Secretariat. (2009), Centralised System to Monitor Communications (CMS Implementation). Press Information Bureau Archive. <https://pib.gov.in>.

³⁰ Centre for Internet and Society (CIS) India. (2014). India's Central Monitoring System: Something to Worry About. CIS Policy Brief Series. <https://cis-india.org>.

³¹ Press Information Bureau (PIB). (2020). Automated Facial Recognition System Approval and Deployment. Ministry of Home Affairs, Government of India. <https://pib.gov.in>.

³² Centre for Internet and Society (CIS). (2021). Decrypting Automated Facial Recognition Systems (AFRS) and Delineating Related Privacy Concerns. CIS India Reports. <https://cis-india.org>.

³³ Sharma, V. (2018). Internet Traffic Surveillance & Network Monitoring in India: Case Study of NETRA. *Network Protocols and Algorithms*, 10(2), 88-104. <https://macrothink.org>.

such as IB and RAW³⁴.

2.1.4. Surveillance Platforms and Infringement of Right to Privacy:

All of the surveillance platforms work jointly by aggregating the data collected in different forms into one particular 360-degree profile, making it a “mosaic surveillance”³⁵. The National Intelligence Grid (NATGRID) works as a central hub that links to the Crime and Criminal Tracking Network & System (CCTNS), which integrates the data of criminal records, immigration, bank records and telecommunications records, etc and frames a large amount of private data³⁶. On the other hand, the Central Monitoring System (CMS) and DRDO NETRA capture all the live activities without requiring any approvals directly from the telecommunications service providers, Internet providers and other agencies³⁷. Further, the Automated Facial Recognition System (AFRS) combines the Data collected by all other Platforms to make mathematical biometric face templates, which finally makes a 360-Degree profile having all the live and private data of individuals³⁸.

Recently, the use of data surveillance platforms was found in the massive protest by the Cockroach Janta Party (CJP) at Jantar Mantar, New Delhi. The affidavit submitted by the Delhi Police at the Supreme Court admitted the use of the Automated Facial Recognition System (AFRS) used via the AI-powered surveillance units “Ikshana” vehicles³⁹. The Solicitor General representing the State stated that the tracking was for “legitimate State interest” to find out the hardened criminals who all participated in the protest. However, the major highlight showing the faulty AI-powered surveillance captured that out of 2,873 individuals having criminal records, 25 individuals were those who were locked inside the Tihar Jail at the time when the protest took place⁴⁰. Such flaws in data surveillance not only infringe privacy but also draft criminal profiles which are arbitrary in nature. If a broader view were taken of the use of

³⁴ *Research Academic Paper Reference*: "Internet Traffic Surveillance & Network Monitoring in India: Case Study of NETRA," Macrothink Journal.

³⁵ Shivangi Narayan, *Smart Policing and the Surveillance State in India* (Routledge 2023) 112–115.

³⁶ Press Information Bureau (PIB), 'Status Report on NATGRID Architecture' (Ministry of Home Affairs, Government of India, 2022) pib.gov.in.

³⁷ Centre for Internet and Society (CIS) India, 'Deep Dive into India's Central Monitoring System' (CIS Policy Series, 2014), cis-india.org.

³⁸ Vidushi Marda and Devdutta Mukhopadhyay, 'Decrypting Automated Facial Recognition Systems (AFRS) in India' (CIS India Reports, 2021) cis-india.org.

³⁹ Krishnadas Rajagopal, 'SC to examine "proportionality" of the use of facial recognition at NEET protests' *The Hindu* (New Delhi, 18 August 2026).

⁴⁰ 'Express Exclusive: Delhi Police Facial Recognition at Jantar Mantar Protest Flags Incarcerated Individuals', *The Indian Express*, (2026), <https://indianexpress.com/article/express-exclusive/delhi-police-facial-recognition-jantar-mantarprotest-accused-in-jail-10862099/>.

surveillance platforms in protests, the right to peaceful assembly is also infringed.

Amongst all of the Data surveillance platforms, the NATGRID, CMS and DRDO NETRA are established through executive orders and are operated without passing a statutory law. The platforms have failed to meet the three tests laid down in the *KS. Puttaswamy vs Union of India* case and further leads to the violation of the Right to privacy. The integration of all private data and constant monitoring of the daily life cycle of individuals raises the question over the democratic accountability and urges judicial intervention, as such a shift, called “functional creep” subjected to using the Data as a weapon against individuals.

III. Government Exemptions and Gaps in the Data Protection Framework

3.1 Exemptions Available to the State under the Digital Personal Data Protection Act, 2023:

The Digital Personal Data Protection Act, 2023 was enacted on a phased basis from August 11, 2023.

The objective of act was for processing the digital personal data in a manner that protects the right of individuals and simultaneously to process such personal data for lawful purposes⁴¹. The provisions of the DPDP Act, 2023 are applicable to all types of industries and businesses that are dealing with personal data; however, the Act exempts all government agencies to oblige with the strict rules as laid down in law. The following are the important provisions that specifically exempt the State:

- (I) Section 5 & 6: Under these provisions, all such private sectors are required to send a notice before processing the private data and obtain consent, which is to be free, specific, informed, unconditional and unambiguous. While notice and free consent are compulsory requirements for private entities, the State is exempted from asking for such consent and notice before recording the private data of individuals and processing it.
- (II) Section 9: Under this section, all the industries processing the personal data of children are banned from tracking and monitoring online interactions, and parental consent is required.

⁴¹ *The Digital Personal Data Protection Act, 2023*, No. 22 of 2023, India Code (2023), <https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf>.

As the State is not under compulsion, the State can directly extract the data from sectors like education and health in the name of protection of public welfare.

- (III) Section 10: Under this section, all the large private entities processing personal data must appoint Data Auditors to conduct the audits, which shall be independent. However, the State agencies are exempted from such restrictions and can collect the personal data of individuals without any periodic independent audits.
- (IV) Section 17: This provision provides information of what all are the exempted from the law. Section 17 is a major loophole that allows the State to misuse its power under this provision to infringe privacy. The section serves as a pathway for State agencies to collect data without any consent and notice from individuals. Under Section 17(2)(a) of the law, the State can exempt any of its agencies from binding the rules and regulations laid down under the law in the interest of national security, public order and sovereignty of India. Thus, if the State allows any of its departments who are dealing with the private data of individuals to skip all the compulsions such as the notice and consent under section 17(1) and then, under section 17(4) that allows the State to keep the data forever and infringe the “right to be forgotten”.
- (V) Therefore, the State agencies which are declared under section 17 can access any private data of individuals without knowing the person and further misuse that data and store it without any safeguards. The major setback behind the said provision is that the individual cannot sue the State for any such actions that violate the fundamental rights of individuals, and thus the infringing has zero independent oversight and does not require any approval by the judge to conduct such actions by the State⁴².

3.2 Statutory Contradictions: Sections 28, 29, and 47 of Aadhaar Act

The constitutional validity of the Aadhaar Act, 2016 was challenged in the *Puttaswamy case*. However, certain provisions still stand and infringe different aspects of the Right to Privacy, which are highlighted below:

Section 28: The provision states that security and confidentiality shall be ensured by the

⁴² Consent in Form, Surveillance in Substance: A Constitutional Critique of India's Data Protection Regime,”LawStreet Journal (August 2026)

authorities that collect all the demographic data and biometric data of individuals for the Aadhaar registration. In the said provision, Section 28(5) does not allow the individual themselves to access their own biometric information. The said section is contradictory to the part of data ownership of individuals and information self-determination. Thus, the provision clearly denies complete ownership by not allowing the access of individuals.

Section 29: Section 29 of the law states about the Restriction on sharing information that is collected under the law. The provision does not allow the State to transfer the biometric data of the individual but fails to erase the footprints remaining of the biometric data that is used for mobile SIM cards, bank account opening and others where the biometric data is used.

Apart from this, the section does not protect the demographic data as locked. The sharing of the demographic data is permission-based, as the State share the Data once permission is given by the individual.

Section 47: Section 47 directly attacks privacy and accountability. As per the section, if there is any case of leaked or stolen data, then the individuals are not allowed to file a lawsuit. The individuals have to rely on and wait till the authorities take action to file the suit and get a remedy.

The above-stated sections of the Aadhaar Act are inconsistent with the privacy standards of India. The law is more inclined towards the government, as the individual loses control over the data and becomes defenceless.

4.2 Broad Grounds of National Security, Public Order and Sovereignty

III. CONSTITUTIONAL PROTECTION OF PRIVACY IN INDIA

3.1 Evolution of the Right to Privacy

1. M.P. Sharma v. Satish Chandra⁴³:

In this case, the Supreme Court examined whether the search and seizure violated the Fundamental Rights under the Constitution of India. The Court ruled that, in comparison to the Fourth Amendment of the US Constitution, the Indian Constitution does not recognise any rights against search and Seizure and further observed that the Right to Privacy is not

⁴³ M.P. Sharma v. Satish Chandra, AIR 1954 SC 300 (India).

recognised as a fundamental right in the Indian Constitution.

2. Gobind v. State of M.P.⁴⁴

In this case, the Supreme Court examined the constitutional validity of police surveillance. The Court stated that the right to privacy could be interviewed between the Article 19 and 21 of the Constitution and further held that the restriction on privacy must be justified based on the public interest, and the law shall be interpreted in a narrow manner to restrict individual liberty. The Court upheld the police regulations that were challenged for constitutional limitations.

3. R. Rajagopal v. State of Tamil Nadu⁴⁵

In this case, the Supreme Court held that the Right to privacy is implied and interwoven in the Right to Life and Personal Liberty under Article 21 of the Constitution of India. The Court stated the Right to Privacy as a “right to be let alone” and held that individuals have the right to protect their matters, which include the Family, marriage and personal life, from unauthorised publication. It further stated that such right is subject to exceptions and limits the State from imposing prior restraint on publication.

4. PUCL v. Union of India⁴⁶

In this case, the Supreme Court held that tapping telephone conversations is a violation of privacy and Article 21 of the Constitution of India. The Court stated that the authorities tapping the conversation shall do so lawfully, just, fair and reasonably, by procedure. Further, the Court amended Section 5(2) of the Telegraph Act, 1885 and laid safeguards including the authorisation by the authority and review of interception orders. The Court established safeguards against State Surveillance via telephonic conversation.

3.2 Constitutional Recognition: K.S. Puttaswamy vs Union of India⁴⁷

Constitutional Recognition: K.S. Puttaswamy v. Union of India (2017)⁴⁸

A nine-judge bench in the case of *K.S. Puttaswamy v. Union of India*⁴⁹ delivered a landmark judgment on an issue involving the collection of citizens' personal information, including their

⁴⁴ Gobind v. State of Madhya Pradesh, AIR 1975 SC 1378.

⁴⁵ R. Rajagopal v. State of Tamil Nadu, AIR 1995 SC 264.

⁴⁶ People's Union for Civil Liberties v. Union of India, AIR 1997 SC 568.

⁴⁷ Justice K.S. Puttaswamy (Retd.) v. Union of India, AIR 2017 SC 4161.

⁴⁸ (2017)10 SCC 1.

⁴⁹ (2017)10 SCC 1.

biometric data, fingerprints, and iris scans.

This case is also known as the “*Aadhaar Card Case*”. The Hon’ble Supreme Court, through this case, overruled *M.P. Sharma v. Satish Chandra*⁵⁰ and *Kharak Singh v. State of Uttar Pradesh*⁵¹, and expressly recognised “Privacy” as a fundamental right embodied under Art. 21 and stated that privacy is a core part of the right to life and personal liberty, and that individuals shall have complete bodily autonomy.

The Hon’ble Supreme Court stated that individuals have an interest in regulating and controlling their private information; however, the government may restrict it only with the restrictions satisfied under the constitutional requirements. The Court, through this case, protected the “Right to privacy” as a fundamental right under Article 21; however, it did not deal with the issue relating to the validity of the Aadhaar scheme.

3.3. Critical Assessment of the Indian Position:

“Privacy” has been a constant issue in India, although the Hon’ble Supreme Court, through the landmark judgment of *K.S. Puttaswamy v. Union of India*, has expressly stated that privacy is embodied under Art. 21 of the Indian Constitution and is an integral part of a dignified life; hence, it is a fundamental right of an individual, protecting their personal privacy, dignity, bodily autonomy and other personal choices overlapping with Art. 19 and Art. 14 of the Constitution.

The Parliament, for the regulation and protection of the privacy of individuals, have enacted the *Digital Personal Data Protection Act, 2023*⁵², and the *Digital Personal Data Protection Rules, 2025*⁵³, in order to process digital data. However, despite these efforts of the Parliament, privacy is one of the most infringed rights of the citizens, as the Government, which should have been the protector of the right to privacy of the citizens, is the one who keeps infringing it, failing to satisfy the reasonable constitutional safeguards provided in the Constitution and discussed in *K.S. Puttaswamy v. Union of India*⁵⁴.

⁵⁰ AIR 1954 SC 300.

⁵¹ SCR (1) 332.

⁵² Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India).

⁵³ Digital Personal Data Protection Rules, 2025, G.S.R. No. 846(E) (India).

⁵⁴ (2017)10 SCC 1.

IV. CONSTITUTIONAL PROTECTION OF PRIVACY IN THE EUROPEAN UNION

4.1 Constitutional Foundation of Privacy

In the European Union, state surveillance is guarded under Article 7 and Article 8 of the Charter of Fundamental Rights⁵⁵. The Articles protect the individual's data, including home, communication and private life and mandate the processing of personal data by fair means and for a specific purpose. The EU Framework under the ePrivacy Directive Article 15(1) states that the EU member states are allowed to pass data privacy laws for national security and criminal investigations; however, such laws shall be applied within the purview of the Charters. The State Authority shall not independently conduct surveillance, as stated in the *Prokuratuur case*; it was stated that even for the purpose of criminal investigation, the authority cannot access the electronics, traffic data and location of the individual and has to first pass the review by a court or an independent administrative body and thereby ruled that a prosecutor's office shall be termed as independent⁵⁶. Moreover, in the *La Quadrature du Net* case, it was held that the mass surveillance of people is illegal and ruled that any such indiscriminate surveillance shall be first authorised by an independent authority or a judge⁵⁷.

The mechanisms and the principle in the EU work hand in hand when it comes to infringing the privacy of an individual. The Court, based on multiple precedents, has clarified that data collection shall be permitted only by an independent judge or authority. However, if the other side of the ruling is observed, the decision clearly restrains the offices from authorising themselves. It distributes the powers and objects to decrease the interference.

4.2 Restriction on Indiscriminate bulk Data retention:

In Europe Union, there are well-defined and specifically dedicated laws that govern the Data Collection and Surveillance systems. These mechanisms of logging and saving the metadata of individuals by internet providers, telecommunication companies and Metadata collectors are strictly termed illegal. Also, such activities by government authorities are termed as illegal based on the Charter and multiple precedents. The Court has ruled multiple times that such activities are to be performed by the government; then it must be targeted, and the bifurcation

⁵⁵ Charter of Fundamental Rights of the European Union, 2012/C 326/02, Art. 7&8.

⁵⁶ H.K. v. Prokuratuur, Case C-746/18, ECLI:EU:C:2021:152 (Mar. 2, 2021).

⁵⁷ *La Quadrature du Net & Others v. Premier minister & Others*, ECLI:EU:C:2020:791 (Oct. 6, 2020).

shall be based on the grounds of a high-level threat or national security.

Further, there are organisational bodies that works for the implementation of the laws. The European Data Protection Board (EDPB) and National Data Protection Authorities (DPAs). The bodies provide guidelines on how enforcement is to take place, and the National authorities keep an audit of how the other State Authorities are working while being under the umbrella of rules and regulations⁵⁸.

4.5 How do all these mechanisms protect from the Government:

- (i) Fishing Expeditions: The regulations do not allow the bulk collection of data, and thus any government agency cannot directly look into the private data of individuals and is restricted from directly tracking all the movements, daily routines, financial transactions and associations.
- (ii) Judicial permission: The regulations do not allow the police authorities to directly search the data. If the authority wants to investigate, then firstly it has to prove before the judges the national threat issue and only after valid permission are such investigations and interventions considered valid.
- (iii) Fruit of Poisonous Tree: If the authority, without any specific permission, comes up with the private data of an individual, then such data would not be considered valid as the mode of collection of the data and medium used is in itself illegal and thus such data obtained illegally shall be used against an individual.

Thus, subject to the jurisdiction of the EU and the law and order, there are proper mechanisms that rigidly protect the interest of individuals by protecting their private data from government surveillance.

V. CONSTITUTIONAL PROTECTION OF PRIVACY IN SWITZERLAND

5.1 Introduction

Swiss laws are well-known for their national policy on maintaining confidentiality. In comparison to Indian law on the right to privacy, Article 13 of the Swiss Federal Constitution

⁵⁸ Regulation (EU) 2016/679 (GDPR), Art. 51.

guarantees the Right to Privacy to every individual and protects the private Data of individuals⁵⁹. Further, based on the expressed provisions, the country has developed other legislation protecting the law over the privacy of individuals. The system has a three-tier process to access the private data of an individual. The three stages are explained hereinafter.

5.2 The “Three-Layer Shield” of Individual Privacy

5.2.1. Layer 1 - Constitutional Protection:

Article 13 of the Swiss Federal Constitution provides an absolute right to privacy to the Individual. This serves as a fundamental baseline through which laws protecting privacy emerge and develop significantly to safeguard private data. The Swiss Constitution protects the private data of individuals' life, family life, house and maintains the confidentiality of communication channels, including telephone and mail. This Right barricades the intervention of the State authorities in monitoring the life cycle, transactions and other private data of individuals, with the help of other statutory legislation developed by relying on constitutional rights⁶⁰.

5.2.2. Layer 2 - Statutory Framework: The Revised FADP

This layer includes the statutory protection by enactment of the Federal Act on Data Protection on 1st September 2023. The law is framed by aligning with the standards of the GDPR of the European Union. The framework mandates the commercial data compliance units at the earliest possible stage to comply with the principles of Privacy by Design and Privacy by Default.

5.2.3. Enhanced Protection for Sensitive Personal Data

The Data that is collected that is not basic, such as health records, political views, and such data that enables the profiling of individuals, is classified as High-risk Data. These Data are not allowed to be directly collected by companies at large. Under the Federal Act, such highrisk data is termed as “Sensitive Data” and cannot be used by companies directly without the explicit consent of the person. Further these of Data iso consented

⁵⁹ *Protection of Data privacy in Switzerland*, Forschungsdaten. Info, <https://forschungsdaten.info/fdm-imdeutschsprachigen-raum/schweiz/protection-of-data-privacy-in-switzerland>

⁶⁰ Swiss Federal Constitution, Art. 13. See also *Proton AG v. Federal Department of Justice and Police*, highlighting the boundaries of telecommunications classification within Swiss constitutional rights.

then a specialised legal hoops shall be passed by the companies collecting the Data to transmit it across borders. The Federal Act shall allow the transmission of such data to other jurisdictions only if such Data are going to be stored on equivalent data security standards as of Switzerland.

5.3 Suing Swiss Authorities for Unlawful Data Extraction:

In Switzerland, the State Authorities need a statutory law or a court warrant to extract Data of an Indian. If the authorities fail to do so and directly collect the data, then the State authorities shall be directly sued by the Individuals. The direct grounds for suing are either the absence of Statutory Law, no explicit warrants and breach of Article 13 of the Swiss Constitution. The individual can file a formal complaint under the Federal Administrative Procedure Act for the stoppage and detention of the Data that are extracted. Furthermore, the Federal Act allows the individual to sue the Authorities if such illegal collection of Data causes financial damages, professional damages or affects the reputation of the person⁶¹.

Thus, that's how the fortress is built up by the Swiss laws to protect the privacy of individuals from the organisations and also from its own government agencies. These organisations work in accordance with the laws and makes the Swiss one of the best countries when it comes to individual privacy.

VI. COMPARATIVE CONSTITUTIONAL ANALYSIS

6.1 Constitutional Recognition and Scope of Right to Privacy:

The European Union and Switzerland have constitutionally recognised the Right to Privacy. In India, there is recognition of the Right to Privacy under Article 21 by constructive interpretation in the case of *K S Puttaswamy*, but the major question is. By just framing the precedents, it safeguards the privacy of individuals against government programs. The EU and Switzerland have proper mechanisms backing the guarantee given under the constitution, while, in comparison to India, there is a clear absence of any mechanisms that check the implementation and enforcement.

⁶¹ Federal Act on the Liability of the Confederation, Members of its Authorities and its Employees (Government Liability Act).

6.2 Legality and Proportionality of State Surveillance:

In India, the collection of information is necessary for national security and to decrease criminal activities. The information that is collected shall be based on the purpose, which must establish the legitimate State aim, proportionality and legality. Also, in the EU and Switzerland, the State shall comply with the legal safeguards that are applicable for the collection of information and surveillance. In comparison, the question arises as to whether the information is solely used by the State for the stated purpose or for other purposes, which was never asked because such information is merged with other information and then used to make a profile. There are multiple sources and different types of information collected by the State through many means, out of which few are justified and are fulfilling the criteria set by the judiciary, but there are certain other unauthorised programs that work behind the scenes and merge all the information and collect the information without any expressed consent or justification. Such work of the State infringes the legality and proportionality of the State, as the State is working *ultra vires* to the safeguard precedents.

6.3 Mass Surveillance, Data Retention and Emerging Technologies:

The surveillance that is performed by the State using high-end and AI-driven technology collects excessive information about individuals, which sometimes leads to function creep. As we saw at the malfunction during the CJP protest, where the facial recognition recorded and scanned faces and linked them to people who were never present there. Such threats of overusing the information with AI-based surveillance are a challenge and shall be overcome by the State first with a guarantee of no misuse and unnecessary harassment to the individual.

6.4 National Security Exceptions and Independent Oversight:

In India, national security is the legitimate exception to conduct surveillance. The State-run programmes work just because of national security and collect information. The accountability of the government always raises concerns, as Section 17 of India's DPDP Act, 2023 provides an exemption from any of the compulsions. India should bring the government offices also under the purview of the compulsions of the Acts and legal principles similar to Switzerland and the EU, where the purpose of collection is to be specified, and once the purpose is served, the authorities are asked to remove and if this is not followed, then they shall be sued.

6.5 Prior Judicial Authorisation vs Executive-Controlled Surveillance:

In the EU, accessing the private information of an individual requires the review of an independent authority. Also, in Switzerland, judicial approvals are required for telecommunications surveillance. Both these countries limit the power of the authority to be immune; however, when it comes to India, things differ. In India, the authorities have to take approvals from the executive and not from any other independent body or judge for collecting information or surveillance. Such powers give unlimited access to the surveillance authorities and allow them to use this power anytime against anyone without any control.

All of these are the drawbacks of the present system of surveillance which are identified and are required to be improved when compared to the EU and Switzerland.

VIII. CONCLUSION

Overall, the whole system of surveillance in India is one-sided and favours the government, while on the other hand it should protect individuals' privacy, which is clearly absent. The different government programs are there but are all opaque when it comes to consented collection of Data and using it for the stated purpose as claimed. The Data which are collected and the surveillance that takes place through different programs have dodged the legal principles and are merging the Data to make a single profile of every individual in the metaverse. Such mass surveillance without any accountability and transparency causes a huge threat of being misused or being used against the individuals themselves.

In such conditions, where the population at large sees the authorities as a protector, the authorities have become a threat, as there is no judicial intervention and they are implemented bypassing the rules and regulations. In India, where there is such an open system requires to borrow similar systems from the EU and Switzerland to make it a natural and independent system of mechanisms and protect the right to privacy of every individual in the country.