AN ANALYSIS OF SURVEILLANCE AND DATA PROTECTION WITH REFERENCE TO THE RIGHT TO PRIVACY

Jyoti Bala, Chandigarh University

& Dr. Amita Arora, Assistant Professor, Chandigarh University

Introduction

"We can trace the "right to privacy" emerging from the two statements of the Preamble, namely "freedom of thought, speech, belief, faith and worship" and "fraternity defending the dignity of the person.."[1] Privacy is a dynamic concept. There is no fixed definition of privacy. Different people have defined privacy differently.

The word "privacy" has been defined as the "individual's rightful claim to determine the degree to which he wishes to communicate with others and his control over the time, place and circumstances of interacting with others. This implies his right to withdraw or to take part as he sees fit. It also implies the right of the individual to monitor the spread of knowledge about himself; it is his own personal possession."[2] Because it is a fundamental right, privacy is not something that can be granted. It is wrong to disregard someone's requests when it comes to showing respect to an entity.

"Judge Thomas Cooley in Olmstead V United States[3] gave the simplest definition of privacy, calling it the right to be left alone," Unlawful use of a person's identity or access to their private affairs, which may give rise to legal action under tort or even constitutional provisions, is what is meant by invasion of privacy.

Right to privacy

Rights are interests protected by 'legislation according to Salmond, i.e. by moral or legal rules. The term "natural right" is applied to rights that are guaranteed based on moral principles, regardless of the legal system in place or the way the law works. As a result, Roscoe Pound

[1] Justice K.S. Puttuswamy (Retd.) V. Union of India, W.P. (C) NO.494/ (2012), pp19-20.
[2] Dr. Sanjib Kumar Tiwari, "Right to Privacy : The Role of Indian Judiciary", JCC Law Review, Vol.III(1), 2012, pp. 10-20 at p.10.
[3] (1928) 277 U.S. 438

views natural law as a philosophy of human moral traits, and natural rights as deductions from human nature that are demonstrated by reason. Individuals' privacy is at risk because of various legal traditions' treatment of the right to privacy. According to Samuel Warren and Louis D. Brandeis, who wrote about privacy in the Harvard Law Review on December 15, 1890, there are various levels to privacy. To achieve these unique characteristics of secrecy, this is what has happened.

a. A right to privacy is the right to be alone. A typical negative right turn indicates that no one else is allowed to get in the way of you running your business.

b. In rem, we find the right to privacy. –.

c. Individuals' inviolable identity is protected by their right to privacy.

Evolution of Right to Privacy: Constitutional Framework

Over 500 pages long and drawing on Indian law and history, the Supreme Court of India's Puttaswami decision from Aug. 24th 2017 declared the right to "Privacy," which could have worldwide repercussions. For this reason, in M P Sharma [(1954) SCR 1077] and Kharak Singh [(1964)1 SCR 332,) the majority followed the majority's substantive attitude in Gopalan [(1954, SCR 1077). Maneka Gandhi v UOI 1 SCC 248 (1978) put an end to this method with its doctrinal proclamation and the judgement in Cooper. Rustom Cavasji Cooper V Union of India4 ("Cooper") 1 SCC 248 (1970) An established constitutional law position has taken the role of the M. P. Sharma and Kharak Singh case law basis for the past six decades. Article 19 of the Universal Declaration of Human Rights declares that the inclusion of particular freedoms as protected rights does not limit Article 21's scope. Other Supreme Court decisions have established the right to privacy as a fundamental constitutional right. These decisions include: Gobind V. Madhya Pradesh State, Rajagopal V. Tamil Nadu State, and the People's Civil Liberties Union V. India Union. According to the Supreme Court, Articles 21 and 19(1)(a) and 19(1)(d) of the Indian Constitution safeguard privacy. Union of India v. Justice K.S. Puttuswamy (Retd.) A table was set up for discussion on UIS and privacy concerns.

One of the shortcomings of India's privacy concept is that it does not exist as a positive right, but is merely a right of resistance to targeted intrusion. The right to privacy, for example, would be useless as a notion of resisting something like generalised street video surveillance as long

as a citizen is not identified as a disadvantage, this right would be of no use. So this privacy right is a detrimental right not to be interfered with.

Laws relating to privacy in India

In August 2017, the Indian government formed a Committee of Experts to research numerous data protection challenges in India, provide precise recommendations on the principles underpinning a data protection policy, and draught such a bill.. This was in response to the Supreme Court of India's Puttaswamy judgement. Personal data of citizens must be secured while the digital economy expands," says a government official.It is predicted to be successful. The right to privacy, which is currently established as a fundamental right in Article 21 of the Constitution, is discussed in detail in Part III. Previous amendments have been made to these two sections relating to private information under the Information Technology (Amendment) Act, 2008..

Section 43A, Security measures for personal data or information and compensation for damages or willful misconduct of the person affected by this act are addressed. Information like passwords, bank account information, credit card numbers, medical records, and biometrics are all instances of extremely sensitive personal data.\.

Section 72A, contract terms that call for imprisonment for up to three years and fines up to Rs.5,00,000 for any individual who causes unjust damage or gain by disclosing another person's personal information while performing services under legitimate contract conditions

2011 Information Technology (Sensitive Personal Data and Information) Rules (Reasonable Security Practices and Procedures and Personal Data) broadly govern the following:—

The act of receiving, holding, using, storing, processing, or otherwise dealing with personally identifiable information.

2011 Information Technology (Sensitive Personal Data and Information) Rules (Reasonable Security Practices and Procedures and Personal Data) broadly govern the following:—

- Information pertaining to an individual's sensitive personal data or information.
- Shared Confidential Personal Data.

- Authentication methods used to protect sensitive personal information from being accessed by others.
- Personal information that should not be sent outside of India is being sent.
- Authentication procedures to protect sensitive personal information.
- Personal data that is particularly delicate may be sent outside of India.
- Personal information that is confidential has been made available to the government.
- Retaining Personal Data or Knowledge.
- Analysis and adjustment of individual details or information.
- Deleting private personal data or removal of consent information.

In spite of the fact that the new digital era or information technology is viewed as the source of privacy issues, we also know that poison killing by poison or iron may cut through iron. In digital space and procedures, there are laws, guidelines, and well-mechanisms that can be used to design privacy preservation schemes. Such as an encryption system to secure sensitive information from unauthorised use in cyberspace

Concept of Surveillance in India: Surveillance laws and judicial precedents

India is the nation's biggest democracy, and its constitution and laws safeguard free speech and expression. However,It's true that freedom of speech and expression on the internet isn't limitless, but for a variety of reasons. Speech and expression can be regulated for a variety of reasons, including defamation, national security, and community cohesion. Article 21 of the Indian Constitution can be used in numerous ways. It also demonstrates that, even now, the majority of Indians lack computer access and materials to support that they are protected from monitoring agencies' clandestine activities.

The need to address the complexity of the digital realm is more pressing than ever. Digitization, which are mostly driven by the private industry and constantly use people's information, are quickly infiltrating contemporary countries' social, cultural, economic, and political structures. Big data and artificial intelligence are becoming increasingly powerful, threatening to create an intrusive digital world in which States and enterprises can observe, analyse, forecast, and

even manage their actions in new and unexpected ways. Data-driven technology is here to stay, but if it isn't handled with care, it poses serious threats to human authenticity, self-reliability, and privacy[4].

Particularly beneficial are these technological improvements. Because of their lack of online and offline access to resources, most Indians today are still safeguarded from covert actions by supervisory agencies. However, the government and the Indian people should not be reassured about this. Close observation of an individual or a group of individuals, especially one who is suspicious of being observed, is what is meant by surveillance. Various technologies are increasingly being used to keep track of cybercrime. Free expression and employment are fundamental human rights that are being violated here. A sense of confusion and disorientation is also created, because when individuals learn that information may be monitored without recourse to norms and regulations, it becomes clear to them that free and open exchange of ideas is no longer possible[5]

Surveillance legislation

IT jobs are plentiful in India, but the country lacks clear laws governing government monitoring. Legislation and regulations controlling surveillance have been established by the legislature, Although laws are needed to ensure that government agencies, their rights, the importance of personal privacy, and freedom of speech are protected. Among other things, the federal government has the authority to intercept, monitor, or decrypt any data on any system resources under Section 69 of the Information Technology Amendment Act of 2008 (the "Act")). But who has the authority to intercept this data remains a mystery.

However, the CERT-In will only be activated and used if an attack on Indian systems or assets or any of India's servers is detected by any foreign company or individual operating in the nation.

The Indian Telegraph Act of 1885 also gave the government the right to intercept any transmission if it was harmful to public security, and successive laws have since granted the

[4] "Surveillance In India", Drishti IAS, 20 July 2021, available at <https://www.drishtiias.com/daily-updates/daily-news-editorials/surveillance-in-india-1>

[5] Chhaya S Dule, K. M Rajasekharaiah and B Prashanth "Analyze The Legislative Framework relating to Surveillance and Right to Privacy: Issues and Challenges", IOP Science, 2020, available at <https://iopscience.iop.org/article/10.1088/1757-899X/981/2/022063>

government the authority[6].

Many distinct laws made by legislation have given indirect powers to the operating governmental entities.

There will be no public access to the data collected by the Central Monitoring System save for government agencies including the Intelligence Bureau, Research and Analysis Wing, Central Bureau of Investigation, National Investigation Agency, Central Bureau of Direct Taxes, and Narcotics Control Bureau (NCB). However, it is unclear who has provided this power or when such surveillance will take place. Although the Indian legal structure has mechanisms for electronic monitoring, they are ineffective.

Also, in 2011, the government introduced the Right to Privacy Bill, in which it attempted to describe privacy, as well as the situations under which the government has the authority to undertake surveillance and the consequences for misusing information gained through monitoring[7].

The Home Secretary, Ministry of Home Affairs, Government of India, has the authority to grant surveillance under this bill.

On October 27, 2009, the central government introduced the Information Technology (Procedure and Safety Guard for Intercepting Monitoring and Decryption of Information) Rules, 2009, which made it illegal to monitor, supervise, or decode computer resources without a written order from the Home Secretary or Joint Secretary, Ministry of Homeland Security (MHA). According to rule four, any organisation may be granted the right to intercept, supervise, or decrypt any data kept on a central government-controlled computer system.

Information Technology (Procedures and Safeguards for Blocking Public Access to Information) Rules, 2009, was enacted by Parliament in 2009. IT Act section 69A (India's sovereignty and integrity, defence, cordial relations with other countries, and state security,

[6] Shivam Gupta and Payal Golimar, "All you need to know about communication surveillance laws in India", iPleaders Blog, 19 September 2021, available at < https://blog.ipleaders.in/all-you-need-to-know-about-communication-surveillance-laws-in-india/>

[7] Apurva Vishwanath, "The laws for surveillance in India, and concerns over privacy", Indian Express, 3 August 2021, available at <https://indianexpress.com/article/explained/project-pegasus-the-laws-for-surveillance-in-india-and-the-concerns-over-privacy-7417714/>

among other things) allows for the blocking of computer resources if they are being used for one of the listed purposes[8].

INDIAN GOVERNMENT FOR SURVEILLANCE

Many new ministries and agencies have been established by the Indian government to monitor internet-related activities, such as personal and business e-mail and mobile phone usage and social media posts. Because of its rapid growth, India must adhere to the best norms and regulations to protect the information technology sector as well as the privacy of all its residents. It has been made possible by organisations such as the National Intelligence Grid and the Central Monitoring System to monitor the internet, cell phone calls and private conversations. Right now, they are not considered to be in charge of body security, which includes the rights and duties of authorities, monitoring circumstances, and data security.

Freedom of Expression The issue is that the term "transmit" has only been established in the context of section 66E.

In sections 67, 67A, and 67B, the word "causes to be transmitted" is used. On the surface, that statement appears to contain both the receiver who begins a transfer and the person whose server the information is delivered from. In India, however, the person charged with obscenity is generally the person who creates and transmits the pornographic material, not the one who consumes it. This new amendment may signal a shift in that viewpoint. Section 66A, Article 19(1)(a) of the Constitution plainly prohibits the government from punishing anyone who sends an unwelcome message. To limit freedom of speech, one must show that the data being used to justify the restriction is clearly linked to civility or moral standards, public order, or defamation (or any of the other four reasons stated in Article 19(2)). This is not always possible, however. Many people believe that the harm principle of John Stuart Mill, rather than the offence idea of Joel Feinberg, provides a preferable framework for freedom of expression. The second half of Section 66A(c), which deals with deceit, is enough to prevent spamming, so the first part, which deals with irritation or discomfort, is unnecessary.

In Shreya Singhal v. Union of India[9], On the basis of Article 19(1)(a) of the Indian Constitution, a two-judge bench of the Indian Supreme Court ruled that Section 66-A of the

[8] PRASHANTI UPADHYAY, " Surveillance in India and its Legalities", Legal services India, available at <http://www.legalservicesindia.com/article/2162/Surveillance-in-India-and-its-Legalities.html>
[9] Shreya Singhal v. Union of India, (2013) 12 SCC 73

Information Technology Act, 2000, which prohibited online expression, was unconstitutional. On the basis of Article 19(2) of the Indian Constitution, the Supreme Court concluded that the section was unconstitutional. Online freedom in India has taken a major step forward since this case.

Remailers, tunnelling, and other forms of online anonymity may be hampered as a result. This does not appear to be the intention of the lawmakers, yet the section may have the desired effect.

As a result, this should be addressed. The Central Government has the authority under Section 69A to "give orders for limiting public access to any information through any computer resource." In English, this means that the government has the authority to restrict any website. While requirement or expediency in respect of particular restricted interests has been established, there are no rules. "Shall be such as may be authorized," according to Section 69-A (2). Before any censorship powers are provided to anyone, it must be assured that they are prescribed beforehand. Any regulation that grants an administrative power unsupervised authority to conduct censorship is clearly irrational in India.

Privacy In India vis-à-vis surveillance

Surveillance is an important instrument for preserving the nation's sovereignty, integrity, and safety, as well as for preventing and investigating these offenses. However, because to the lack of a data protection statute that covers the millions of monitoring measures, the government has unrestricted access to residents' private lives. Following that, nine Supreme Court judges held in K.S. Puttuswamy Vs. Union of India[10] privacy is guaranteed by the Indian Constitution under Articles 14, 19, and 21, which means that it cannot be broken except in the interest of defending the state's integrity and sovereignty. Legally, if it wasn't 2017, the current state of affairs about whether or not privacy is an Indian Constitutional "fundamental right" was in question.

Despite the fact that citizens' right to privacy has been deemed a basic right, law enforcement authorities can conduct interceptions and monitoring simply by delegating authority, with little to no oversight of their operations. In the sphere of national defense, there is no potential for judicial review of these measures when they are approved, and also because the individuals

[10] K.S. Puttuswamy Vs. Union of India, (2017) 10 SCC 1

under surveillance would not be aware that they have been being observed, neutralising any possibility of objection to the orders.

As a result, the government's interception and monitoring authorities are now being deployed according to its personal whims. The lack of a Data Protection Act isn't helping matters[11].

Surveillance and privacy

While the potential of cyber-terrorism is very significant, indiscriminate traffic monitoring is not the method to go if you want to obtain results, and it will almost certainly backfire. A needle is considerably easier to locate in a little bale of hay than in a haystack. Rather than receiving information overload from impeded surveillance of massive amounts of data, small-scale and focused monitoring of metadata (also known as "traffic data") is a far more effective way that will really lead to consequences. If such protections are not in effect, the powers may be questioned as to their legality due to a lack of supervised application[12].

JUDICIAL INTERPRETATION

Prior to the Supreme Court of India's decision in Justice K.S. Puttuswamy and Ors. v. Union of India (UOI) and Ors.[13], That's why people didn't believe privacy to be a fundamental right. As a result of this decision, Article 21 of the Indian Constitution was revised to incorporate a right to privacy. The verdict overturned M.P. Sharma v. Satish Chandra[14], District Magistrate, Delhi, and partially overturned Kharak Singh v. State of Uttar Pradesh[15], both of which argued that the Indian Constitution does not recognise the right to privacy as a fundamental human right. In this decision, Justice D.Y. Chandrachud feels that an individual must live with dignity, and that privacy is one of the requirements for any human being to live a decent life, as well as an essential part of achieving the goals and objectives that the preservation of life and liberty was made to accomplish. He also believes that if a law infringes on a person's privacy, The Indian Constitution's fundamental rights must be adhered to. If there is a breach of privacy, it

[11] Shashwat Singh, "Surveillance In India Post The Right To Privacy Judgment", Legal Services India, available at <https://www.legalserviceindia.com/legal/article-2273-surveillance-in-india-post-the-right-to-privacy-judgment.html>
[12] Jitender K Malik, Sanjaya Choudhury, "Privacy and surveillance : The Law relating to Cyber Crimes in India" 9(12) Journal of Enginering, Computing and Architecture (2019)
[13] K.S. Puttuswamy Vs. Union of India, (2017) 10 SCC 1
[14] M.P. Sharma v. Satish Chandra, 1954 SCR 1077
[15] Kharak Singh v. State of Uttar Pradesh, 1964 SCR (1) 332

shall be justified under Article 21 on the grounds that a legislation allowing such a breach must provide a mechanism that is just, fair, and reasonable.

If there is a breach of privacy, it shall be evaluated under Article 21 on the grounds that a legislation allowing such a breach must provide a mechanism that is just, reasonable, and equitable. He outlined a three-part test for any legislation that sets a mechanism for privacy violations. A law can be considered valid if it passes this three-part test.

The following are the three prerequisites[16]:

1. Legality, which assumes that there is a law;

2. Necessity, as determined by a valid governmental goal;

3. Proportionality ensures a sensible relationship between the objectives and the methods employed to achieve them.

"Informational privacy was a component of the right to privacy," he makes the argument.

The current Court advises the Union Government to investigate and implement a comprehensive information privacy framework. Individuals and the state's legitimate interests must be carefully balanced in order to implement such a system. A legitimate goal of the state is to safeguard national security, prevent crime, promote innovation, and regulate how public benefits are distributed. These were policy issues that the Union government needed to address when creating a well-structured data protection regime. ” As a result, if the government must conduct surveillance on somebody, the surveillance must meet the three-fold standard, and the balance must be preserved.

Only where there is a compelling government interest and there is a very immediate need to pry into somebody's privacy could the right to privacy of that person be violated, according to Justice Jasti Chelameswar.

A violation of Article 19(1)(a) of the Indian Constitution is a violation of the right to freedom of speech and expression, which is harmed by monitoring. The Supreme Court of India came

[16] Chhaya S Dule, K. M Rajasekharaiah and B Prashanth “Analyze The Legislative Frameworkrelating to Surveillance and Right to Privacy: Issues and Challenges”, IOP Science, 2020, available at <https://iopscience.iop.org/article/10.1088/1757-899X/981/2/022063>

to the conclusion that People's Union for Civil Liberties v. Union of India[17] infringes Article 19's(1). (a) right to free speech and expression if any individual is tapped on the phone [18].

State of Haryana v. J.R. Gangwani[19]: On the basis of sending e-mails to customers of the Company using fictitious email accounts that contained content that tarnished the Company's reputation and was required to be provided by the Company Law Board, Section 66-A(c) has been filed for review. Misdirected customer emails were delivered to the complainant's inbox. Section 66-A(c) requires emails to be sent to the complainant or the corporation, however the defendant and petitioner both claim that this was not the case. "The petitioners are delivering these communications to the buyers of cranes from the business, and such consumers cannot be regarded to be prospective buyers of the company," the High Court ruled.

As a result, delivering such e-mails is not encouraging the sale process, as stated in the advertisements in the Economic Times. As a result, such advertising are intended to disturb or bother the firm, or to mislead or confuse the addressee about the source of such advertisements. As a result of these facts, In my opinion, the petitioners' conduct clearly violates section 66A(c). Police Research and Development in Hyderabad has handled a number of high-profile cyber investigations, including the analysis and extraction of material from a laptop confiscated from a terrorist who assaulted the Parliament.

The BPRD's Computer Forensics Division received a laptop that had been taken from two terrorists who were shot dead in Parliament on December 13th, 2001, after Delhi's tech experts struggled to identify most of the data on it. The laptop had a fake ID card with the Indian government's seal and insignia, as well as a Ministry of Home sticker that the terrorists had planned to put on their ambassador car. This offered further evidence of their motives. The three lions' crests were scrutinised in great detail, and a seal was made with great care, including the precise location of Jammu and Kashmir.

CONCLUSION

The significance of data and privacy can be found across every element and circle of human life, whether it is in business management, in which the SWOT (Strengths, Weaknesses,

[17] People's Union for Civil Liberties v. Union of India, AIR 1997 SC 56
[18] Shivam Gupta and Payal Golimar, "All you need to know about communication surveillance laws in India", iPleaders Blog, 19 September 2021, available at < https://blog.ipleaders.in/all-you-need-to-know-about-communication-surveillance-laws-in-india/>
[19] State of Haryana v. J.R. Gangwani, (Crl) No(s).1878/201

Opportunities, Threats) Analysis is based primarily on data compiled by your competitors, or in the health or legal sectors, where data plays a comprehensive and absolutely essential role in deciding whether the outcomes are in favour or against the individual or entity at large.As a result, it is not incorrect to call privacy and data "A Determining Element" of successfulness of any individual, organization, or company in today's world, and the same is true for a state. If a state wishes to develop, the right to privacy and data protection should be a top priority. In terms of internet policy, India is a key member. The Indian government is eager to establish itself in democratic data regulation as a worldwide leader, and it has been successful doing so to a significant extent[20]. Proposal of data protection legislation in support of constitutionally-protected privacy is a tiny step toward becoming a global leader in democratic data governance. However, the bill's language seems to be primarily a basic combination of GDPR provisions with an authoritarian inclination. Furthermore, the ambiguity of the distinction between non-personal and personal data remains a source of worry. The bill ultimately weakens security for individual data rights through allowing the government to retrieve whatever it deems appropriate under the established exclusions.

By introducing the Personal Data Protection Bill of 2019, India has definitely taken a step forward to enacting a comprehensive framework regulating the data protection in the country. Data fiduciaries' responsibilities for handling personal data are outlined in the bill. In addition to establishing more stringent penalties for infractions, it also includes provisions to protect the privacy rights of individuals whose personal information is being processed. The Bill mandates that organisations be registered with the state as data fiduciaries in order to process the data[21]. The law not only addresses data protection and privacy, in addition to M & A and other strategic and financial investments in India, such as minority and majority stakes, especially software, artificial intelligence, pharmaceuticals, hospitals, etc. It also impacts potential investments in data-intensive targets. , E-wallet and financial sector. Foreign companies operating in India and involved in the processing of personal data must bear equal responsibility under the bill. Data trustees have been given extra responsibilities for the transfer of personal data outside of India under this bill. The proposal is a huge step forward for the country's data protection framework, and if passed, it would tie both state and private businesses. However, there are several grey areas in the Proposal that the state must resolve.

[20] Jayanta Boruah & bandit Das, "RIGHT TO PRIVACY AND DATA PROTECTION UNDER INDIAN LEGAL REGIME" 1 DME Journal of Law (2020)
[21] Saharsh Saxena, "Right to Privacy and The Personal Data Protection Bill of 2019: A Critique" India Law Journal (2020)

Users are not adequately protected under the bill against certain injuries or damages. Rather than identifying and regulating such behaviours, the laws focus on establishing precautionary obligations. Furthermore, there is no defined classification of essential personal data, and it is up to the National Government to notify it. The provisions governing cross-border data transfers are likewise weak.The government has taken a number of unjustified authorities, such as providing federal agencies a relief from the Bill's provisions. Furthermore, during this present Covid-19 pandemic, the whole planet's attention is focused on online services and the utilisation of the internet. Also the Government of India has prescribed a model for e-governance and e-courts, with the first phase of online filing currently underway for the e-courts establishment[22]. Online platforms like Zoom and Google Meet allow people to work from home, while e-classrooms allow kids to learn from the comfort and privacy of their homes. When 80% of the country is operating through the Internet, whether the children are attending online classes or the adults are doing work from home, there will definitely be a significant increase in data privacy violations in the country. The government should address these issues related to privacy and data protection as their top concern.

However, The right to privacy has been elevated to the status of a fundamental right in India by a number of judicial decisions. However, if we look at our current situation, we can see that globalisation has resulted in a massive technological advancement. And, with the digital revolution, the issue that remains is whether or not we enjoy privacy in our lives. This right is a crucial component of living a decent life, making our own decisions, and developing ourselves, so it is quite vital. As it can be seen in the present era, technology has become an essential part of our lives it has benefited us greatly, but it has also become a potential danger since with the advancement of technology, several more problems such as cybercrime, data leaks, information theft, and other issues have arisen, all of which have a direct connection to our privacy. As we all know, in order to obtain any types of service, we are required to share our information and private details with a third party (private or state)[23]. However,Even if the country has many laws and regulations that indirectly control data protection rather than directly, sharing such personal data and information raises the risk of breaches or abuse of data because of the lack of sufficient Data Protection Laws. Just a few examples include the Information Technology Act, Criminal Law, Intellectual Property Law, and so on. A 'Breach

[22] Mandeep Kumar and Puja Kumari, "Data Protection & Right to Privacy: Legislative Framework in India" 7(11) Journal of Critical Reviews (2020)
[23] "Surveillance In India", Drishti IAS, 20 July 2021, available at <https://www.drishtiias.com/daily-updates/daily-news-editorials/surveillance-in-india-1>

of Privacy' can occur if such information is released or abused illegally by a third party. Many loopholes can be found in existing laws, such as for the internet, providers of service, data intercessors are not accountable for any infraction of data processing if they can prove that such data was processed without their knowledge, so to protect data privacy we need a stringent Data Protection Law. According to the Supreme Court's decision in Art. 21 of the Constitution, privacy is an inherent right that cannot be violated. However, simply having this viewpoint is insufficient because one must be informed of one's rights as well as the choice of going to a greater authority for justice if those rights are violated[24]. It is possible that they could be left unclothed if they were unknown. When people are well-known for their rights, they can progress or enjoy a decent life. Previously, solely personal privacy was taken into account, but this has changed over time. This means that the government should implement an effective system that can notify them so that they can act fast. Aside from that, legislators should adopt legislation that ensures the security of the collected data. Databases that store information require strict security measures to prevent even professionals from accessing them, but they can only be accessed by those who have permission to access them, which is also beneficial to the citizens of the country. Furthermore, only those agencies responsible for data collection, processing, and storage should be held fully accountable[25]. Furthermore, every law must include a penalty clause, such as monetary and imprisonment penalties, that are sufficiently severe to make an unauthorised person think long and hard about abusing personal data. Some analysts have recommended that instead of collecting health information, smart cards be used, which would be a voluntary option. Since biometrics are authorized to recognise persons despite when they do not want to be recognized, smart cards that use passwords will need individuals' deliberate co-operation during the recognition procedure. No one can use smart cards to recognize anybody once they've been discarded. Foreign governments might use a collection of biometrics to recognize Indians if smart cards were adopted, which would eradicate or at minimum lessen the risk of criminals and terrorists.

[24] Chhaya S Dule, K. M Rajasekharaiah and B Prashanth "Analyze The Legislative Framework relating to Surveillance and Right to Privacy: Issues and Challenges", IOP Science, 2020, available at <https://iopscience.iop.org/article/10.1088/1757-899X/981/2/022063>

[25] Jayanta Boruah & bandit Das, "RIGHT TO PRIVACY AND DATA PROTECTION UNDER INDIAN LEGAL REGIME" 1 DME Journal of Law (2020)