iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** VIII **Month of publication:** August 2025

DOI: https://doi.org/10.22214/ijraset.2025.73824

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VIII Aug 2025- Available at www.ijraset.com

Privacy and Data Protection in India's Legal Framework

Sanjay A. Mulik[1], Dr. R K Gupta[2]
Research Scholar, NIILM University, Department of NIILM University, Kaithal

Abstract: ***Globally, privacy has become a fundamental human right, and the Indian Constitution recognizes it as such under Article 21. As society digitizes, along with technological advancements, safeguarding personal data and privacy has become increasingly difficult. In India, privacy rights have been acknowledged through judicial interpretations and legislative measures, such as the Information Technology Act and the proposed Digital Personal Data Protection Bill, but comprehensive protection against data misuse and breaches remains a challenge. In this paper, we examine the evolution of privacy as a legal right in India, analyze the existing legal framework, and discuss its limitations. The study compares India's approach to data protection with international standards such as the European Union's General Data Protection Regulation (GDPR). The report emphasizes the necessity of robust mechanisms to ensure accountability, secure sensitive information, and address emerging privacy concerns in the digital age, improving the legal framework for privacy and data protection in India.***
Keywords: Privacy, Data protection, Personal Information, Sensitive Information, Confidentiality;

I. INTRODUCTION

An individual or a group of people can maintain privacy by concealing and restricting their information. Furthermore, it has been recognized globally as a fundamental right under Article 12 of the Universal Declaration of Human Rights, which states that everyone has the right not to be impeded in his privacy, correspondence, and family, and not be allowed to slander its honor or standing. Every individual has the right to be protected from such interruptions. Common liberties treaties specifically recognize privacy as a right. Similar language was embraced by the ICCPR, the ICPRAMW, and the IJNCRC. It is necessary for Data Protection Regulations to be in place to ensure this Right of Privacy. In addition, such Regulations are classified as "that heap of privacy regulations, methods, and arrangements that strive to reduce infringement on one's privacy caused by the collection, collection, and conveyance of personal data.". In addition, Individual data refers to data by which a person's personality can be known, regardless of whether it is gathered by an element or government."

The concept of privacy has a long history, it is a part of the Human Rights which are inherent to every human being from birth. There can be no sacrosanctity, no division between them. This right includes the right to be left alone, the right to have privileged communication, the right to privacy of the body, the right to have a sexual orientation, the right to have a family, etc. Nevertheless, it excludes private information, information of public interest, and public records. It is very important to maintain privacy in order to live a dignified life. Nevertheless, with the advancement of innovative technologies and the wide use of internet, it has become much easier to access anyone's data and to share it with third parties, resulting in misuse. Our society is also subject to many cybercrime attacks, including phishing, viruses, ransomware, hacking, spamming, etc. Therefore, we need strict Data Protection Laws to prevent such attacks. Despite the absence of comprehensive data protection laws in India, the Constitution of India, the Information Technology Act 2000, the Indian Contract Act, and Intellectual Property Laws are used to enforce data protection. Moreover, the IT (Amendment) Act, 2008 was passed in order to address all the issues not covered by the original law.

A couple of very important provisions have also been inserted, via Sections 43A and 72A, which essentially discuss the obligation of corporate bodies to disclose data when they infringe on contracts. Also, many efforts are being made to protect data, including amending the IT Act, the Data Protection Commission of India, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data and Information) Rules, 2011, and the Data (Privacy and Protection) Bill, 2019. Possibly it is not the first time that Parliament has been presented with a Data Protection Bill; Baijayant Jay, a member of Parliament, had introduced a bill in 2009, the Prevention of Unsolicited Telephone Calls and Protection of Privacy, that sought to limit unwanted telephone calls made by individuals or business promoters to people who explicitly expressed opposition to receiving them, yet continued to call uninterruptedly. Aside from Baijayant Jay, many other legislators have introduced bills relating to the privacy of citizens in the past, including Rajeev Chandrasekhar (2010), Om Prakash Yadav (2016), etc.

Although the Bill of 2019 has not yet been enacted, it is expected to do so soon. In addition, many of the issues came into consideration after the Supreme Court declared the privacy judgment in the case of K.S Puttaswamy, including whether Aadhaar Act (Targeted Delivery of Financial and other Subsidies, Benefits, and Services) Act 2016 is valid, as well as Section 377 of the IPC, which refers to consensual homosexuality.

The illegal sharing of data, whether it is personal or sensitive, is now the basis for earning income for those who illegally share data. Also, it has been alleged that offshore companies have exported people's data from India through offshoring operations. There is a major threat to privacy as a result of these factors. To determine whether the Indian Legal Framework is sufficient to ensure the privacy of Indian citizens, or whether new provisions need to be adopted, this article will analyze the Indian Legal Framework. To gain a better understanding of the requirements in Indian legal system to ensure a higher level of data security, this paper will further examine some of the international legal instruments adopted by foreign countries.

II. INDIA'S EVOLUTION OF THE RIGHT TO PRIVACY AS A FUNDAMENTAL RIGHT

There is no explicit definition of privacy in the Constitution. But generally speaking, privacy refers to the right of a human being to live freely without disturbance, the right not to be interfered with as well as the right to be left alone. Nevertheless, many people are exploited from enjoying this right, and many others are even unaware that it is their right that can never be taken away from them. Therefore, many Declarations and Covenants have been enacted to raise awareness of people's privacy rights. Under Article 21 of Part III of the Constitution, the Indian Judiciary has also interpreted privacy as a fundamental right. In the following series of cases, the right to privacy was addressed –

A. MP Sharma v. Satish Chandra

In this case, the power and seizure provision was challenged on the basis of a violation of the Right to Privacy. It was, however, observed by the higher judicial authority that the Framers of the Constitution did not intend to limit the power of search and seizure as a violation of fundamental privacy rights. Additionally, the SC clarified that MP Sharma's case did not resolve the question of Right to Privacy as a Fundamental Right under Part III of the Constitution. As a result, the Right to Privacy is not a Fundamental Right under the Constitution.

B. The State of Uttar Pradesh v. Kharak Singh

Surveillance under the UP regulation was questioned on the grounds that it violated Part III of the Constitution's Fundamental Rights. The Supreme Court struck down Regulation 236(b) as a violation of ordered liberty and an unauthorized intrusion on a person's home because it permitted surveillance by night visits. In spite of this, the other clauses of the Regulation were still legitimate since Privacy was not yet recognized as a fundamental right under the Constitution. According to J. Subha Rao, privacy is an integral part of Article 21 even if it is not recognized as a fundamental right.

C. The case of Govind v. the State of Madhya Pradesh

The MP police regulations 855 and 856 were again challenged in this case on the basis that state surveillance at night at the residences of habitual offenders and picking up whom they suspected to be criminals violated the right to privacy. SC, however, refused to strike down these regulations, holding that domiciary visits at night are not always unreasonable restrictions on the right to privacy. In this case, the Supreme Court held that the right to privacy cannot be enjoyed in its entirety. On the basis of compelling public interest, fair restrictions could be imposed.

D. This case relates to Malak Singh Etc. v. The State of Punjab and Haryana

It was held by the Supreme Court that where there was no illegal interference, State surveillance exercised within its limit and without violating the citizen's right to personal liberty, was valid and lawful.

E. The State of Tamil Nadu vs. R. Rajagopalan

In the case of R.Rajagopalan, the higher judiciary, by declaring the right to privacy intrinsic in Article 21 of the Constitution, determined that every Indian citizen has the right to safeguard his or her privacy whether it pertains to education of child, giving birth to and raising a child, reproduction, decision regarding marriage, family. It is illegal to publish anything regarding the above topics without the permission of the person concerned, regardless of whether the statement is genuine, complimentary, or critical. This is a clear violation of privacy if someone does so."

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VIII Aug 2025- Available at www.ijraset.com

F. A case between the People's Union for Civil Liberty and the Union of India

In this case, the right to privacy was violated through telephone tapping, which was questioned as constitutional. According to the Supreme Court, the right to privacy includes talking over the telephone and such calls can be made whether at work or at home since telephone conversations themselves form an integral part of man's life. Article 21 of the Constitution protects against the invasion of privacy through the monitoring of telephone conversations. A law directing the procedure to be followed for telephone tapping, or rules framed under the Telegraph Act, may permit the State to tap such conversations.

As a result of this judicial interpretation, different kinds of privacy were created, such as privacy of telephone conversations and privacy of medical records. Although majority judges in both Kharak Singh and MP Sharma cases held that Right to Privacy is not a fundamental right, it has not been declared as such.

A petition was filed in 2012 by K S Puttaswamy challenging the constitutional validity of the Aadhar Act for violating privacy. Thus, 9 judges of the bench examined the new matter of whether the Right to Privacy is a fundamental right while leaving aside the validity of the Aadhar Act that was later heard by a five-judge bench. So, in Puttaswamy case, the Supreme Court overruled the earlier judgments of Kharak Singh and MP Sharma cases by declaring that Right to Privacy is an intrinsic part of Part III of the Constitution, which is intrinsic to Article 21 itself.

Based on the above discussion of all the cases, we have concluded that Right to Privacy is now declared to be a Fundamental Right under the Indian Constitution.

III. CONCERNING PRIVACY ISSUES

The Aadhaar judgment in respect of privacy raised many issues including: Constitutional validity of the Aadhaar Act, Section 377 of the IPC, live-in relationships without marriage, etc., which can be briefly summarized as follows:

A. The Aadhaar Program

Indian citizens can benefit directly from the Aadhaar scheme launched by the Government in 2009. This unique identity can be used to prove identity as well as to access government welfare services like LPG distribution and Jan Dhan Yojana. UIDAI issued a 12-digit number to all Indians by obtaining demographic information (name, address, sex, etc.) and biometric information (iris scan, finger print, etc.).

A number of grounds were raised to challenge this scheme, including:

- In the first place, it was governed by an executive order rather than a statute;
- A second problem is that data will be collected by private agencies without any provision for data security;
- Lastly, no prosecution is available in cases where data is mis-used or is not used for the purposes for which they were collected.

In 2016, the Lok Sabha passed a money bill known as the Aadhaar Bill, which becomes an Act thereafter. The main purpose of the Act is to provide legislative support for the Aadhaar scheme. Aadhaar was linked to PAN, phone number, bank account and other services after its enactment. In pursuance of Aadhaar, many petitions were filed challenging its Constitutional validity based on the infringement of privacy before the Supreme Court, which was heard by five judges, including Dipak Mishra, Justice A.K. Sikri, A.M Khanwilkar, Ashok Bhushan, and D.Y. Chandrachund. According to a recent ruling by a majority of 4:1, the Aadhaar Act is constitutionally valid. Nonetheless, the court struck down several provisions such as Sec. 57, Sec. 47, and Sec. 33(2); this means that private entities cannot ask for Aadhaar numbers, and individuals can now file complaints against entities and the government. According to J Chandrachud, one of the five judges, the Act violates part III of the Constitution, making it unconstitutional. Aadhaar was considered a fraud on the Constitution because it was passed as a money bill, undermining the Rajya Sabha and thus contradicting the Constitutional scheme.

B. According to Section 377 of the Indian Penal Code (IPC),

In accordance with IPC, Section 377 reflects unnatural sex, and the Delhi High Court dismissed Naz Foundation's application in relation to Section 377. Nevertheless, in 2009, the HC of Delhi decriminalized homosexual acts between consenting adults after 8 years. In 2013, however, it repealed the judgment of the High Court of Delhi in the case Suresh Kumar Koushal v Naz Foundation.

On July 10, 2018, after many petitions were filed, a five-judge bench led by CJI Dipak Mishra heard the case again, decriminalizing homosexuality by partially striking down the colonial era provisions of Section 377 of IPC. Essentially, the higher judicial authority argues that sexual relations constitute a right to privacy, which is protected under Article 21 of the Constitution, which guarantees the Constitution's Right to Life and Personal Liberty. On the other hand, the State can impose reasonable restrictions if there is a compelling public interest.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VIII Aug 2025- Available at www.ijraset.com

IV. THE INDIAN LEGAL FRAMEWORK ON THE RIGHT TO PRIVACY

As of now, there is no specific legislation that deals with privacy and data protection in India. Although there is no such legislation, there still exists a legal framework which indirectly addresses privacy and data protection, though not directly. Privacy is also protected under the Constitution of India, in addition to statutory protection. In essence, privacy rights and personal data can be protected by two mechanisms.

A. Protection under the Constitution

Neither the Constitution nor the Declaration of Independence expressly or implicitly recognize privacy as a Fundamental Right. There is no mention of it in the Constitution. According to Article 21 of the Constitution and Part III of the Constitution, it is an integral part of the Right to Life and Personal Liberty. It has been recognized as a Fundamental Right in the Puttuswamy case by a nine-judge bench, but it cannot be fully enjoyed. Under Article 19(2), rational limitations such as public interest, sovereignty, and integrity of the nation can be imposed.

We have been granted the right to privacy since birth, which is also an inalienable right. Its relevance can be gauged from the fact that even if the Supreme Court, by its majority decisions, held that Right to Privacy is not a Fundamental Right, minority opinions of many judges from the beginning argued that it is a Fundamental Right under Article 21 of the Constitution. Article 21 is considered the core of the Constitution because it incorporates many rights that are essential to give constitutional recognition to newly emerging rights as the society's needs change.

B. Protection under the law

Data protection laws in India include the IT Act, 2000, Indian Contract Act, 1872, Intellectual Property Laws, and Credit Information Companies Regulation Act, 2015, which are described below in brief:

1) The 2000 Information Technology Act

In India, the IT Act, 2000 is the first ever legislation addressing e-commerce, e-governance, and cybercrime. Additionally, it is the legislation that deals with data protection. As a result of leaks of information from computers, the purpose of the IT Act is to protect information from infraction. Among its provisions are: Sec. 65 and Sec. 66, which prevent others from illegally using technology like computers, laptops and information.

- Section 43 of the IT Act punishes any destruction of computer data. A person who uses computer data illegally or in an unauthorized manner will be sentenced to 3 years in prison or a fine of 5 lakhs rupees, or both.
- Section 65 protects anyone who alters, destroys or conceals computer source code knowingly or intentionally.
- Under Section 66, anyone who alters or damages information stored in a computer will be held liable. A person who violates these sections is liable for 3 years imprisonment or a fine of Rs. 2 lakh, or both.
- Additionally, if a company violates the IT Act, its managers and directors are personally responsible.

To address the issues that the original Act lacked coverage for and to assist further development of IT and related security concerns, the 2008 Act was enacted. Under Section 69(A) of the new Amendment Act, the Indian government is empowered to prevent interceptions, monitors, and decryption of computer systems, resources, and electronic data. Later in 2015, the Supreme Court declared that Section 69(A) under which the government can order the blocking of internet sites is constitutionally valid since it provides adequate procedural safeguards.

2) The Indian Penal Code of 1860

Violations of data privacy are not directly criminalized in criminal law. A violation of privacy can be inferred from certain crimes, for instance, under Article 408 of the IPC liability arises from dishonest misappropriation of property.

3) The law of Intellectual Property

For copyrighted piracy (theft), the Copyright Act, 1957 imposes mandatory punishments in proportion to the seriousness of the offense. Section 65 of the Act stipulates that any person who uses a computer or a copy of an infringing computer program may be imprisoned for up to three years or fined. In addition, where an author collects information from different sources by devoting time, money, labor, and skill, that amount to literal work within the meaning of the Copyright Act and are protected as their copyright. Consequently, the outsourcing parent entity may have recourse under the Copyright Act in the event of a violation of that data base.

4) CICRA

According to CICRA regulation, any information relating to an individual's credit must be collected in accordance with privacy norms. In the event that the entities modify or divulge the collected information, they will be held responsible as outlined in this regulation. The entities that collect and maintain data are held responsible if their data is leaked or altered. A strict structure has been framed by CICRA in India to protect information regarding credit and tenancy of companies as well as individuals. In addition, these principles have been assessed by the RBI as being stringent for information privacy.

5) The Indian Contract Act of 1872

According to Indian law, the Indian Contract Act, 1872 governs contractual terms and agreements generated by the parties. It is therefore legally permissible for parties to enter into a contract that includes a confidentiality or privacy clause, which means that personal information of individuals can only be disclosed with their permission and consent, and only for a purpose or in a manner that is agreed upon by the parties. A person who discloses information in an unauthorized manner and fails to comply with the expression stated in the contract is in breach of contract and can be sued for damages as a result. Furthermore, in an insurance contract, the insurer provides a proposal that contains confidential information about the customers of the insurer. If such information is disclosed without their consent, they may be liable for damages under a contract they have agreed upon.

V. RECENT EFFORTS IN INDIA TOWARDS DATA PROTECTION

In light of an increase in data theft and breaches of privacy, the government as well as the business sector needed to do something for the protection of data regardless of their legitimate structures. Here are a few examples:

A. An Amendment to the Information Technology Act is Proposed

The Service of Correspondence and Data Innovation proposed specific changes to the IT Act, 2000 in regards to data protection. A result of these ideas was the IT (Revision) Act, 2008, which further consolidated significant arrangements related to Data Protection, such as Segment 43A and Segment 72A. These arrangements are both correctional and common, for example, for lawbreakers and common criminals. However, this is in accordance with the IT Act. As this recommended revision is presently not sanctioned into another arrangement under the equivalent, another set of rules has been outlined named Privacy Rule.

These Principles were broadcast by the Service of Correspondence and Data Innovation under Segment 87 (I) (06), which discusses sensible security practices and systems to be employed while handling delicate individual data. As a result of resistance to these Guidelines, activity will be drawn into Segment 43A of the said Act, which will force responsibility to pay remuneration. However, its cutoff points have not been determined.

These Standards contain only arrangements related to sensitive individual data or information (SPD). SPD stores credit/check card data, secret words, biometrics (like a unique finger impression, Deoxyribonucleic Acid, and so forth), as well as physical, mental, and physiological medical problems. Moreover, these Guidelines specify that any data contained in the public space and accessible to the entire population without much expense, is not to be expressed as SD?

These Guidelines also specify that the body corporate or some other individual for the body corporate should handle, gather, and share any private delicate data or information using sane security systems. It is possible that the corporate body may be able to pay remuneration to an individual who suffered harm as a result of the explanation of the infringement of information.

These Principles provide an alternative methodology to regulate data protection in India. The arrangements of these Principles are divided among three gatherings. The following are among them:

- A body corporate is an organization
- Provider of data
- A public authority.

B. The Following Are The Most Important Standards

A decision 4 states that the body corporate commits to implementing a privacy strategy on its website that will be accessible by all suppliers sharing their data, including individual and sensitive information. In addition, the strategy should specify the kind of data collected, the reason for the collection, etc. The body corporate is required to comply with rules 5 concerning the collection of data. I understand some of the points - first, the body corporate will not collect sensitive individual data until and unless the supplier consents and has been informed about the reason for collecting such data.

A legal justification must also be provided for the collection of both personal and delicate data. Furthermore, the data collected from the supplier should only be utilized for the referenced reason and should not be held longer than necessary. For any disagreement between the body corporate and the supplier, the body corporate will get the gathered data and decide which complaint redressal body to use. It is expressly stated in Decide 6 that before the body corporate can expose sensitive data to outsiders, it must get the consent of the data supplier. It is nevertheless possible for the body corporate to share the supplier's data with the public authority offices without its prior approval, assuming that there are regulations that allow outsiders or public authority organizations to obtain such data from the supplier without its earlier consent. In compliance with Control 8, the body corporate will take on and implement sensible security practices. One of the security practices is explicitly listed as ISO security standard, but there is no firm decision on whether it should be adopted. In addition to the previously mentioned code of practices, other codes can be implemented provided the public authority endorses the equivalent. Additionally, the code should be reviewed yearly by an autonomous inspector who is approved by the public authority.

C. Indian Data Security Chamber

As NASSCOM has established a self-administrative body through Data Security Gathering of India, the business can foster proper data privacy and protections principles on its own, since they have a better understanding of common sense business issues than public authorities do. As a non-profit organization, it has sufficient representation of free chiefs and subject matter experts. A DSCI member can likewise be an IT-empowered services organization, an exploration foundation, or an academy that has arose with data security and privacy concerns.

D. Administrations shouldn't be contacted by the public

Since the development of telecom specialist CO-OPS and the easy availability of cell phones, individual privacy of phone numbers became an issue among individuals and businesses in the new past of India. Due to it, numerous spontaneous calls were made to the people by business advertisers or people who would prefer not to receive such calls. Telecom Administrative Power of India (TRAI) has therefore established a Public Don't Call Register whereby phone salespeople cannot call endorsers whose numbers are enlisted.

E. A Bill to Protect Individual Data in 2019

As another late effort towards data protection, Mr. Ravi Shankar, Clergyman of Gadgets and Data Innovation, introduced a Bill in the Lok Sabha on December 1, 2019. In the Bill, Ravi Shankar sought to draft a data protection system to address recent concerns and legal protections. Besides this, there were likewise data protection bills presented to Parliament in 2017 and 2018 as well.

VI. NEED OF SPECIFIC PRIVACY LAWS

Regardless of the current legitimate system and efforts made by the public authority, the current regulations are ineffective in protecting individual privacy rights. Furthermore, a few escape clauses should be added to the current regulations like the Information Technology Act, Rules of 1981, etc. These are some of the reasons why unique regulations may be requested:

In the current legal system, there are certain provisions

1) Incorporating Segment 48A and Area 72A into the IT Act would not have made any new modifications to the first IT Act since anything that comments the Standing board of trustees gives to the Service of Parliamentary undertakings is simply received by them and no application is made.
2) Furthermore, the proposed change does not address the issue of data protection, for example, how to handle sensitive individual data, what safeguards should one take into consideration during the time spent gathering data, handling individual data, etc.
3) According to the MCIT, the guidelines were called "2011 Rule, under Segment 87(2) (06) read with Area 43A arrangements with sensitive data. They apply just to body corporate or individual situated inside India.
4) They don’t consider State authority inside its extensionion. Other than not consenting to the guidelines, summon Segment 43A, which will also accommodate both risk and pay. As far as how much or breaking point is concerned, it hasn't been determined yet.
5) For instance, Vodafone India Restricted, Bharti Airtel Restricted are required to provide their privacy strategy on their websites under Rule 4 of 2011 Guidelines. In any case, hardly any State-claimed areas do not publish their privacy policies on their websites. Due to this, there is no mention of their privacy strategy on their website, which demonstrates a feeble approach to data protection by specialists, and the need for standards is then raised.

6) Starting around 2011, Rule manages delicate data or information (SPDI), such as passwords, clinical records, biometric data, etc. As a result, India has fewer guidelines on non-touchy data. In addition to this. Further, the appropriateness of restricting extraterritorial wards in particular circumstances remains unclear under Indian regulations. As an example, it is unclear whether the IT Act or the Privacy Rules apply to a US organization that gathers SPDT from Indian residents when they depart.
7) Additional constraints that hinder Indian law's ability to protect data include the following:
8) In terms of confidentiality rights, there is no far-reaching regulation.
9) There is no legitimate arrangement regarding private, public, and delicate information.
10) A lack of legitimate techniques for handling, sending, and streaming data.
11) The terms Data Quality, Correspondence, and Data Straightforwardness do not have any legitimate rules to define them.
12) Lack of a legal structure for managing cross-country data streams.

From the above gaps or provisions in the current legal structure, one may conclude that a special privacy and data protection regulation is needed right away. As a result of the tremendous expansion in client support among corporate entities who obtain different customer data, it is also essential to have a comprehensive data protection law. Despite, such expansion in various data advances, web administrations, web in the global space, and expansion of BPO (Business process rethinking) administrators, it becomes crucial to have rigid regulations on data protection that could manage both the movement of data across public boundaries as well as provide sufficient shields to protect the progression of data.

VII. CONCLUSION

Due to a few translations made by the Legal Executive, the Right to Privacy has become a Fundamental Right in India. However, if we observe our current situation, we will find that globalization has led to enormous mechanical advancements. In addition, with the advancement of innovation, a question arises: do we have privacy in our everyday lives? In order to proceed with an honorable existence, to make a choice of our own, and to foster ourselves, such a right becomes essential.

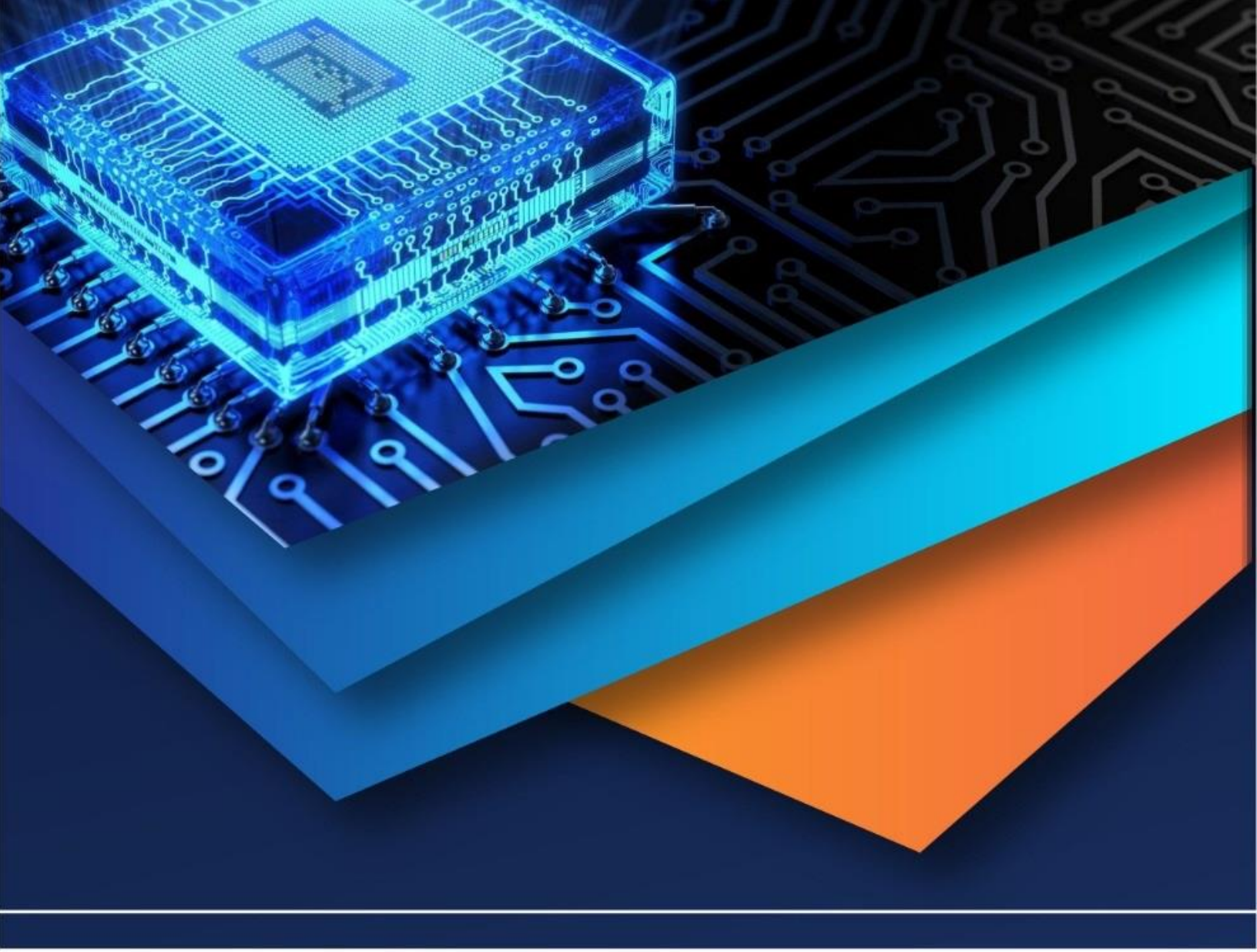
As we can see in this day and age, innovation has become a part of our daily lives, which has benefited us generally. However, it has also turned into a danger, as numerous issues have developed with the advancement of technology, including cybercrimes, data theft, data abuse, and so on, which directly affect our privacy. As we probably are aware, that at present we need to impart our own data or data to a party whether it could be an Administration or confidential substance to profit any sort of administrations, while sharing such data might build the gamble of data burglary or abuse of data on the grounds that in India there is an absence of satisfactory Data Protection Regulations despite the fact that it has specific regulations which however not straightforwardly yet in a backhanded manner is managing Data Protection. Among these are the IT Act, Criminal Regulations, and Protected Innovation Regulations. An outsider's wrongdoing in spilling or abusing such data is often treated as a breach of privacy. Further, numerous escape clauses should have been included in the current regulations, such as those for web administration. As data mediators are not responsible for data handling violations if they demonstrate that the data was handled without their knowledge, we need a severe Data Protection Regulation to protect data privacy.

A fundamental right natural to privacy has been established by the High Court in Craftsmanship 21 of the Constitution, as we are probably aware. However, merely having this perspective is not sufficient, because one ought to know one's rights, and if those rights are violated, one should know that the more significant position can be accessed for redress. In the event that they were not discovered, they may go unrepressed. People can create or have a noble existence only when they are notable for their rights. In the past, only private privacy was considered, however with time it became important to consider data privacy as well. The Public Authority should, therefore, embrace such a productive system that allows them to act as quickly as possible. Besides this, councils should establish specific principles, guidelines, or regulations that can confirm that the gathered data are true. The database where the data is stored ought to be outlined with tight security that, in any case, for the specialists it becomes difficult to get to it, which means it may only be accessible to those with the authority to do so, and that too for the government's assistance. Additionally, only those who gather, cycle, and store data should be made more aware. Furthermore, any regulation should include a punishment system, such as monetary and detention penalties, that is so severe that the unapproved person reconsiders misusing others' data.

Few experts recommend using smart cards as an alternative to collecting biometric data, which would be a discretionary option. As biometric data is permitted to perspective people regardless of whether they constitute recognized, brilliant cards that require pins will ask residents to cooperate during the ID cycle. Discarding brilliant cards makes it impossible to distinguish between people. Using brilliant cards would reduce the risk of crooks and psychological militants, unfamiliar government using biometric data to recognize Indians.

REFERENCES

[1] Atulsingh, Data Protection: India in the Information Age, 59 JILI 78 (2017).
[2] Bijan Brahmbhatt, Position and Perspective of Privacy Laws in India, available at http://www.lawctopus.com/academike/postion_perspective_laws_india/.
[3] Dr. Payal Jain & Ms. Kanika Arora, Invasion of Aadhaar on Right to Privacy: Huge Concern of Issues and Challenges, 45(2) Indian I.L.R. 33 (2018).
[4] Kasim Rizvi & Ranjit Rane, High Time India Had a Right to Privacy Law: A Private Member Bill Tabled Recently Ticks Most of the Boxes That One Would Expect from a Strong Data Privacy Law, LIVEMINT, available at http://www.livemint.com/opinion/eoRER0qfjdocTiTwFzdVJfHigh4imindia-had-a-right-to-privacy-law.html.
[5] Krishnadas Rajagopal, Section 377 Will Not Apply to Consensual Same-Sex Acts, Says Supreme Court, The Hindu, available at http://www.thehindu.com/News/national/section-377-will-not-apply-to-consensual-same-sex-acts-say-supreme-court/article24878751.ece.
[6] Latha R. Nair, Data Protection Efforts in India: Blind Leading the Blind, 4 I.J.L.T.I. 23 (2018).
[7] Rukhmini Bobde, Data Protection and the Indian BPO Industry, 2 Law Rev. GLC 79 (2002-03).
[8] S.S. Rana & Co. Advocates, India: Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, available at www.mondaq.com/India/data/information-technology-reasonable-security-practices.
[9] Shrikant Ardhapurkar, Privacy and Data Protection in Cyberspace in Indian Environment, available at https://www.researchgate.net/publication/50273874/Privacy-and-Data-Protection-in-Cyberspace-and-Indian-Environment.
[10] Soni Mishra, Justice Chandrachud: The Lone Dissenting Voice in Aadhaar Judgment, The Week, available at https://www.theweek.in/news/justice_chandrachud_lone_dissenting_voice_aadhaar_judgment.
[11] Vaibhabi Pandey, Data Protection Laws in India: The Road Ahead, STNGHS & Associate (2015).
[12] Vijay Pal Dalmia, India: Data Protection Laws in India—Everything You Must Know, available at www.mondaq.com/India/data-protection-laws-in-india.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY