International Journal of Law and Public Policy
Vol. 1, Issue. 2, June 2025, pp. 36~47

Data Protection and Privacy

Yash Bhushan
Student Ll.M (Corporate and Securities Laws)
Pondicherry University, Puducherry, India.

Article Info

Article history:

Received Mar 9, 2025
Revised Apr 20, 2025
Accepted May 11, 2025

Keywords:

Data Protection
Privacy
Right
Committee
K.S. Puttaswami

ABSTRACT

"Privacy is not something that I'm merely entitled to, it's an absolute prerequisite." – Marlon Brando

Online privacy for individuals is considered a pipe dream. The act of stopping big commercial tech companies along with the government from gathering and disseminating user data online in order to create a surveillance state is known as data protection. When the right to private was proclaimed a basic right by the Supreme Court in the Puttaswamy case, it completely changed the definition of privacy in India. In order to protect people's privacy, India also needed new laws.

Srikrishna Committee was established for making of such data protection regulations in the nation and responded with a draft measure called as the Consumer Data Protection measure, 2019, which the Parliament has not yet approved. It is founded on the European rules, which are among the most stringent data privacy legislation globally.

The bill gives certain rights such as right to access, verify, ratify, alter, forget, etc.—all of which are crucial in the modern world. This essay gives a summary of the significance and necessity of data protection, the government's actions in this area, official reports on the subject, and considering the relationship between data protection and privacy in light of the Supreme Court's ruling.

Corresponding Author:

Yash Bhushan,
Student Ll.M (Corporate and Securities Laws),
Pondicherry University, Puducherry, India.

1. INTRODUCTION

It is hard to avoid technology in this day and age; in fact, our reliance on it is growing daily to the point that it has surpassed practically every area of security and anonymity. Every day, a lot of data is generated online, and the majority of it is personal information like the things people have purchased online, the locations they have visited on vacation, etc. Since most items can now be accessed on a smartphone, the internet has undoubtedly made our lives easier, but it has also opened the door to a whole new level of privacy violations. Companies like Google and Facebook frequently utilize this personal information to identify connections, identify interconnections in all spheres of human behaviour, impact, control, and further promote their products by following their procedure.

"This data tracking has ease of storing information and using it for personal advantage has become a problem for the public policy that is why it needs to be regulated with stringent laws. It is rightly said that privacy is a myth in this era of technology. Right to privacy in India is protected by the right to life and personal liberty that is under Article 21 of the constitution of India and was recently recognised in the judgement of Justice K.S. Puttaswamy". This verdict forced the Indian government to acknowledge that the Digital India effort would only be successful if the government ensured the security of citizens' particular data and that special legislation were required to implement the initiative because none were in place safeguarding citizens' privacy. Consequently, the government established the "Justice Srikrishna Committee,"

a panel of specialists headed by Justice B.N. Srikrishna, to examine and suggest modifications to India's data protection regulations and provide updates to the relevant authorities. “white paper was also issued along with committee report on data protection ‘A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians’ was submitted along with the draft law which is the personal data protection Bill, 2018”.

Recent incidents include the Indian Aadhaar card scandal, Facebook CEO Mark Zuckerberg's U.S. challenge, Google's alleged tracking and use of personal information, and a documentary on Netflix" The Social Dilemma" have demonstrated the need for regulation and protection of consumer information from large tech companies on a global scale. Regarding data protection, the United States and the European Union hold divergent views. “The EU, at leading the way for global data protection norms has recently implemented the EU GDPR, which has come into operation on 25 May 2018 for the protection of data. While The US follows a laissez-faire approach and does not have a full framework for data protection framework but has a sector specific legislation for it and even the US courts recognize the right to privacy of citizens in this regard”.

This essay gives a summary of the significance and necessity of protecting personal information, the government's actions in this area, official reports on the subject, and the connection between privacy and data protection in light of the Puttaswamy ruling of the Honourable Supreme Court.

As the Internet of Things expands, more information-sensing devices are being connected to the network in order to identify the relationships between individuals, devices, and "things." By 2025, there will be 42.6 billion "things," or an internet of things, according to a recent IDC prediction, generating 76.4 zettabytes (ZB) of data. Additionally, there is constant work to improve the efficiency of IoT device information collection.

The amount of data generated and hosted by the cloud outsourced platform is astounding. The cloud's scalable, reliable, and high-performance servers will host a multitude of smart city apps and services. Additionally, because of the pay-as-you-go feature, most traditional businesses actively migrate files to the cloud. In addition to being a place for burden, the cloud offers effective operational procedures that increase an organization's flexibility and mobility. This has aided in the development of networking and the digitalisation of businesses. The 2019 Global Digital Economy Report from the United Nations states that the digital sector is becoming a more important driver of economic expansion. Cloud storage is essentially a subset of the cloud-based technology that makes online data archiving and sharing possible. Among the benefits of cloud storage include remote backup, easy, safe, and efficient file access, limitless data storage capacity, and affordability. Cloud data in practical applications can be divided into five categories: private, romantic, secure, electricity or mixed form, and active cloud storage.

In the public cloud, companies hire storing companies to manage their data storage requirements, sparing them the headache of server maintenance and infrastructure setup. The information can only be viewed by those who have permission.

Numerous small and medium-sized businesses are drawn to public cloud due to its benefits, which include cost savings, scalability, and flexibility. Personal cloud, sometimes referred to as mobile cloud storage, is really a subset of public cloud, even though it offers free cloud storage offerings to individual customers. Businesses that employ private clouds must assign qualified personnel to construct cloud storage platforms and manage and maintain servers. This ensures that the company's private cloud is greater secure than the general-purpose cloud and that the company itself manages information. However, the price goes up significantly. This storage strategy works better for large organizations that handle a lot of expensive and sensitive data. All of the advantages of both public and private clouds are combined to create hybrid clouds. Companies can store other data in public clouds and sensitive and expensive data in private ones. The use of this storage method is growing in popularity. The financial and medical industries benefit greatly from community cloud, a new cloud storage technique that has emerged in recent years. A neighborhood cloud provides cloud services to several businesses within a locality. Usually, these businesses must work together on specific projects or have related problems. Members of Community Cloud have the option of hiring a third party to manage the servers and construct the infrastructure, or they can collaborate to do so.

The main cloud systems Generally speaking, from the perspective of storage architecture, offer three primary types of storage: blocks, document, and object management..

1) Cloud block storage is suitable with the storage area networks and offers a virtualised SAN with physical volume management provisioning through an easy-to-use web services interface.
2) Network- Attached Storage technology is typically linked to file storage, also known as file-level or files-based storage. Compared to block storage, file storage offers greater control over who can access and share data saved on the file system.

Expanding storage space, data sharing, effective transmission, pricing, and data security are just a few of the issues that firms face when dealing with massive data. When information retention surpasses the PB level over time, NAS and SAN limitations directly raise equipment maintenance costs. Because object

preservation is becoming more and more important, they are unable to completely satisfy the enterprise's needs for dependability, mobility, security, and and other measures of mass storage competence. Using spiders like Shodan, which help attackers look for linked vulnerable devices on the Internet, makes it simpler to identify vulnerabilities in various healthcare system components. Similarly, it is possible to transfer a spreadsheet containing millions of entries of user health data in just one second without leaving any consistent traces.

To safeguard data and user privacy, Policies pertaining to data privacy and protection are in place for the Internet of Things. The anticipated outcomes of these legislative frameworks have not been achieved, and the current state of healthcare data privacy protection falls short of what is needed to address the aforementioned problems. Furthermore, healthcare privacy laws lack a defined set of principles for safeguarding IoHT data due to several constraints and gaps.

2. RELATED WORKS

Interest in the relationship within artificially intelligent systems (AI) and data privacy has grown significantly in recent years, a symptom of a better comprehension of the intricate relationship between legal needs and technological innovation. This section provides a comprehensive review of research that focusses on significant findings, comparative analyses, and recent advancements in AI-driven handling of data. It also highlights substantial contributions and ongoing discussions that are influencing the area. Simultaneously, technological developments have become essential instruments for balancing the development of AI with strict data security regulations. Federated learning, developed by Google researchers, preserves anonymity and locality while enabling collaborative model training across scattered data sources. Because this decentralized method reduces the privacy dangers connected to centralized data repositories, it is especially appropriate for delicate industries like healthcare and banking.

A new technology called the "Internet of Things" assists consumers by exchanging data with other devices that are connected to the Internet. The Internet of Things (IoT) is an internet of sensor devices that can connect with their surroundings, according to the International Telecommunications Union (ITU). Applications such as military usage, remote surveillance, appliances control, safety and other electronic devices are all included in the broader meaning of the Internet of Things. The Internet of Healthcare Things, that is intended to monitor, store, or transmit medical data, is one of the main applications of IoT in the healthcare industry. To put it briefly, IoHT is a subset of IoT that focusses on hardware, services, and healthcare and includes software. IoHT refers to uniquely identified devices used in the medical field that are connected to the Internet and can communicate with one another. By creating clinical data and sending it to a distant server or service over wireless network infrastructure, IoHT devices assist in monitoring people's health. IoHT devices can be recognised by their IP address, just like any other Internet-based device. By connected to the network in this manner, they are capable of transmitting data to and from designated devices. The central server keeps track of this information and reacts appropriately to identify the patients' conditions. By enabling doctors and medical personnel to stay in touch with their patients, the goal is to deliver reliable, effective, and economical healthcare services.

Data flow participation, authorization, and permission of the carried out activities, such as data collecting, retention, processing, and transfer, can provide data privacy, which is thought to be a fundamental requirement for client acceptance. Data privacy hazards are directly related to practices of unauthorized collection, use, accessibility, conservation, and exchange. These acts could lead to user privacy breaches and personal data leaks because healthcare data is very sensitive and valuable, and it has multiple priorities. In this regard, appropriate safety measures and precautions are required. Furthermore, privacy issues are brought on by the availability and accessibility of private medical records online. In June 2015, malware initiated a censorious privacy breach attack by exploiting vulnerabilities in blood gas analyzer devices to gain access to hospital networks and divulge personal data. Despite this, patients ought to have access to current information regarding the privacy framework for IoHT devices and amenities, which should ensure patient data security. The majority of the data is gathered by the healthcare systems from sensor devices and sent to the management layer via intermediary devices. To reliably exchange data throughout this process, a number of mechanisms and encoders are employed.

The idea of privacy, which seeks to preserve individual integrity and dignity, is connected to personal data protection.Because personal data is an asset with significant economic value, its collection and dissemination is a violation of privacy.In Indonesia, direct marketing strategies, especially in the area of credit card management, have made use of customer personal information that has been exchanged through agents without the owner's consent. A bank lost over Rp 250 million as a result of a fraud card case handled by Imam Zahali (IZ), which involved utilizing a customer's debit card for cash swipe transactions. For IDR

800,000 for 25 data, he bought the clients' information online. He pretended to be a debit card salesman when he approached the victims, who were clients, and offered to raise their credit card limits.

Regarding the protection of personal data, Article 28G of the Republic of Indonesia's 1945 Constitution is the highest law.18. A number of laws, including those pertaining to banking, telecommunications, consumer protection, people law, constitutional law, population management, technological information about transactions law, public information publication law, medical law, and other pertinent laws and regulations, governed privacy and personal data protection prior to the promulgation of Law No. 27 of 2022 involving Personal Data Protection (PDP Law) on October 17, 2022.There are now more thorough methods for protecting personal data thanks to the PDP Law.

Statistics Protection and Importance of Privacy

"The term data is mentioned in the Information Technology Act, 2000 as a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer"; the safeguarding of a user's personal information from businesses or the government that collect it, as well as ensuring that all authorizations are obtained and that the user maintains control over the information and can edit or delete it, is known as protecting information or information confidentiality.

Laws are necessary to protect data because there are many private regulators on the internet, whether they are in the taxi industry, food delivery, internet shopping, or other social networking sites. In order to utilize their services, all of these businesses require your phone number, email address, or other personal information. These details may be preserved and sometimes even forwarded to other websites without the user's permission, which is a harm to their privacy in some manner or one. Search history and other data are used by websites like Facebook and Google to recommend advertisements and generate purchases, which is inherently deceptive.. Who granted these businesses permission to exploit private people's data without their consent is the matter at hand.

"Privacy is the right to be left alone or to be free from misuse or abuse of one's personality. The right of privacy is the right to be free from unwarranted publicity, a life of seclusion, and to live without unwarranted interference by the public in matters with which the public is not necessarily concerned". The idea of privacy has been evolving throughout time. It is a very complicated process that is hard to define exactly, and its complexity can be determined by the reality that the harms caused by invasions of privacy are hard to measure because they are primarily intangible. Reputation information is also linked to privacy; it may include details about a person's body, sexual orientation, or other areas they are wary of. "No one shall be bound by willful interception with his privacy, family, home, or correspondence, or to attack upon his honor or reputation," according to Article 12 of the Human Rights Declaration of the Universal. Everyone has the right to legal defense against these charges or attacks"

"Data protection and privacy are connected with each other in a way that data protection principles are specifically made to protect the personal information of users by overlooking on how much information is collected, disclosed and used and since Right to Privacy is an established fundamental right now and because of large use of personal information through electronic or automated means, right to privacy has developed into many jurisdictions. Thus right to privacy and data protection both ensure that personal information about individuals should not be available to other individuals and organisations"..

Today's secrecy issue is complicated by the fact that most internet businesses are private, profit-driven organizations that have access to customer data. Without the user's approval, these businesses will share that information with other private corporations, which is considered a privacy infringement. Consider the following scenario: after conducting a Google search for a product, it is observed that the product begins to show up as commercials on every online platform, including Amazon, a shopping website, and Facebook, where the user is casually browsing. This continues until the user purchases the product that he has searched for. They can only do this by sharing information among oneself, which gives the companies an unfair edge by affecting their users' thoughts. For this reason, the government has to impose regulations to give users significant control over their information and how it is used. Threats to privacy do not only come from non-state actors; the state also interferes in citizens' relationships with the state, which has more power over citizens' lives through harsh and coercive measures like punishing citizens, using police force, placing citizens under surveillance, intimidating them, and violating their personal information".

This tracking of an individual's data is detrimental since the information is inaccurate and may be very deceptive, and the third party gives the personal information to other businesses for very little money without the subject's consent. But it also offers a lot of advantages, including as helping the state keep the peace and track down murderers.

3. THE GROWTH OF DATA PROTECTION LAWS AND PRIVACY RIGHTS OVER TIME

Understanding the monitoring of data surrounding a person is detrimental since the information is inaccurate and may be very deceptive, and the third party gives the personal information to other businesses for very little money without the subject's consent. But it also offers a lot of advantages, including as helping the state keep the peace and track down murderers. This section explores the historical forerunners, landmark occasions, and legal turning points that have influenced the evolution of privacy and data security rights over time.

o History of Privacy Rights: The idea of privacy has a lengthy history and has developed in tandem with cultural customs, societal conventions, and technical breakthroughs. The foundation for early ideas of privacy was laid by ancient societies like the Greeks and Romans, who prized individual liberty and solitude. But it wasn't until the Enlightenment that the idea of privacy started to be incorporated into laws, as intellectuals and thinkers like Jeremy Bentham and John Locke defended it as a vital component of personal freedom.

o Data Protection Laws' Development: Governments and businesses began gathering more data and conducting more surveillance as a result of the 19th and 20th centuries' industrialization and bureaucratic growth. Early data protection regulations were created in response to worries about the exploitation of personal data and the need to preserve individual privacy. One of the first instances is the 1890 Harvard Law Review article by Samuel Warren and Louis Brandeis, which laid the groundwork for the modern right to confidence in the United States. This legal recognition of data protection and privacy rights was reinforced by subsequent legislative efforts, including the 1950 European Convention on Human Rights and the U.S. Fair Credit Rating Act of 1970.

o Legal Turning Points in Data Security and Privacy: Due to worries about consumer rights, government monitoring, and technological advancement, privacy regulations and laws proliferated throughout the second half of the 20th century. Important turning points in the establishment of oversight organizations like the US Federal Trade Commission (FTC) and the enactment of landmark legislation like the US Privacy Act of 1974 and the EU Data Protection Directive of 1995 marked the growth of safeguarding data and privacy regulations. These legislative initiatives established guidelines for gathering, using, and disclosing of personal data in a world growing more digitally connected, laying the foundation for contemporary data protection laws.

o International and Integration Efforts: New security and privacy issues were brought about by the development of the internet and the worldwide interchange of information. In response, regional blocs and international organizations started to standardize data protection rules and practices to protect individual privacy rights while facilitating cross-border data courses.

o Global data protection standards and common principles have been established through initiatives like the European Union General Data Protection Regulation (GDPR) in 2018 and the Office for Economic Co-operation and Development's (OECD) 1980 Privacy Guidelines.

o Continuing Difficulties and Changing Frameworks: In the digital age, many issues still exist despite tremendous advancements in the creation of data protection legislation and privacy rights. Big data growth, artificial intelligence, and rapid technology breakthroughs provide new data security and confidentiality problems. Concerns like algorithmic bias, surveillance capitalism, and the economic worth of personal information also emphasizes the need for constant innovation and attention to detail in the area of privacy laws and policies.

o The development of data protection laws and rights to privacy over time offers important insights into the direction of privacy governance and the difficulties presented by the digital era. We can better comprehend the intricate interactions between social values, technical advancements, and regulatory reactions by following the evolution of privacy concepts and legal frameworks across time. The lessons of the past provide a framework for developing a more just, open, and rights-respecting approach to protecting and preserving data in the twenty-first century as we negotiate the challenges of the digital age.

International Data Security and Privacy Law Frameworks

The international legal framework for safeguarding and safeguarding data is one of the most crucial components of the supervision of personal data in the current day. This section examines important international treaties, rules, and accords that set rules and guidelines for safeguarding privacy rights and controlling cross-border data processing.

o United Nations Resolution and Statements: Through a number of resolutions, treaties, and declarations, the UN has been instrumental in establishing standards and principles pertaining to data protection and privacy. The right to privacy is recognized as a fundamental human right in Article 12 of the 1948 UN Declaration of Human Rights.

- The right to privacy and the significance of safeguarding personal information are further affirmed by other treaties like the International Covenant on Civil and Political Rights and the Internacional Covenant on Economic, Social, and Cultural Rights.
- European Union Regulations and Rules: To preserve people's right to privacy, the European Union (EU) has taken the lead in creating extensive data protection laws. A historic legislative move that creates consistent data protection standards among EU member states is the General Data Protection Regulation (GDPR), which went into effect in 2018. Organizations managing private information are subject to strict regulations under the GDPR, which include clauses pertaining to permission, data reduction, and the ability to deletion.
- Cross-Border Information Transfer Contracts: As data transfers grow more globalized, cross-border communication agreements are becoming crucial for enabling the legitimate interchange of personal data while guaranteeing sufficient security. Legal foundations for the transfer of Mechanisms such as the EU-US Privacy Shield and Standard Contractual Clauses (SCCs) facilitate the transfer of personal data from the EU to other nations that may not have comparable privacy laws. These agreements aim to strike a compromise between safeguarding people's right to privacy and enabling data transfers for business purposes.
- Conventions and agreements on regional data protection have been formed by regional organizations alongside to international treaties to handle data protection issues within their jurisdictions. For example, the Council of Europe's Convention for the Protection of People with regard to Automatic Understanding of Specific Information, or Tradition 108, establishes standards for safeguarding personal data and calls on member states to cooperate in enforcing data protection laws.
- Bilateral and Global Treaties: Enabling data transfers and advancing the harmonization of data protection standards are additional important functions of multilateral and bilateral relationships between nations. These agreements could contain clauses pertaining to information exchange, reciprocal legal aid, and collaboration in the fight against international cyberthreats. Examples include international agreements on counterterrorism cooperation and Mutual Legal Services Treaties (MLATs).
- International legislative frameworks for privacy and security of data offer crucial tools for encouraging uniformity, unity, and collaboration in the cross-border regulation of personal data. These frameworks help to safeguard privacy rights and foster confidence in the global digital economy by defining uniform principles and norms. Effective multinational data governance is still severely hampered by issues like jurisdictional disputes, unequal enforcement, and technological complexity. In order to maintain the efficacy and applicability of regional data protection regimes in a world that is becoming more interconnected, future initiatives to improve interoperability, simplify compliance procedures, and fortify regulations will be essential.

National Data Safety and Privacy Laws

The legal framework governing confidentiality and security of data in each nation is greatly influenced by national laws. This section highlights important regulations and regulatory actions while examining the varied strategies used by different countries to handle the issues raised by the gathering, use, and treatment of personal statistics.

- Data security and privacy are governed by a patchwork of state and federal laws due to the fragmented regulatory structure in the United States. Federal regulations like the Health Insurance Interoperability and Accountability Act and the Privacy Act of 1974 protect private information held by government entities and healthcare providers. The banking and internet industries are also subject to sector-specific rules, such as the Gramm-Leach-Bliley Act and the Act protecting children's online privacy. However, because states have enacted their own privacy laws, such as the Virginia Citizen Data Protection Ordinance and the California Consumer Privacy Act, the lack of comprehensive national privacy laws has led to a fragmented regulatory environment.
- Because the regulatory system in the fragmented United States, state and federal laws governing data security and privacy are patchwork. Private information held by government organizations and healthcare providers is granted rights and safeguards by federal laws including the Health Insurance Portability and Accountability Act and the Privacy Act of 1974, respectively. Sector-specific laws, such as the Gramm-Leach-Bliley Act and the Act safeguarding children's online privacy, also apply to the banking and internet sectors. The absence of broad government regulations on privacy, however, has resulted in a fragmented regulatory environment as states have passed their privacy laws, such as the California Consumer Privacy Act and the Virginia Consumer Data Protection Ordinance.
- Member States of the European Merger: The GDPR, which is standardized in all member states, governs data protection in the EU. The GDPR lays out guidelines for processing identifiable information, including standards for lawfulness, accountability, and the rights of data subjects. In order to supplement the GDPR and provide for certain exemptions or derogations, member states must pass national legislation. In

order to address particular privacy issues within their borders, a few EU nations have also passed sector-specific laws or added protections.

- The primary law pertaining to privacy is the Personal Data Protection and Digital Documents Act and data protection in Canada. PIPEDA establishes guidelines for how private sector entities involved in business operations must gather, utilize, and share personal data. Within their respective territories, provincial legislation like the British Columbia Private Data Protection Act and the Alberta Personal Information Protection Act offer extra protections for personal data. Additionally, the federal and municipal privacy commissioners in Canada are essential in upholding privacy regulations and looking into complaints pertaining to privacy violations.
- Emerging Countries and Growing Nations: Emerging economies and developing countries may have quite different privacy and data protection laws in terms of their application, enforcement strategies, and compliance. Some nations may have insufficient or inexperienced regulatory systems to handle the intricacies of digital data governance, while others have passed extensive laws based on international norms. Furthermore, there may be obstacles to the efficient application and enforcement of privacy legislation in these areas due to elements including a lack of funding, technological capability, and political stability.
- Global norms in the areas of data security and privacy, technical breakthroughs, and changing societal attitudes are all reflected in legislative trends and new laws across jurisdictions. A greater emphasis on data localization, stronger accountability and transparency standards, and more stringent enforcement measures to deal with data breaches and privacy violations are some of the major developments. Furthermore, the advent of new technologies like biometrics and artificial intelligence has forced politicians to review current laws and rules to make sure they are still applicable and effective in defending individuals' right to information in the digital era.
- The global regulatory environment for data protection and privacy is greatly influenced by national laws. Although the breadth and rigor of the strategies used by various nations may differ, the basic objective is always the same: to reconcile the protection of individuals' privacy rights with the benefits of innovations fueled by data. In order to guarantee consistent and reliable protection for private information across borders, efforts to integrate and reinforce national privacy laws will be crucial as technology advances and global data flows become more intertwined. National laws can help create a more just and privacy-preserving digital society by encouraging openness, responsibility, and trusting.

Regulatory Difficulties and Compliance Systems

For people and businesses alike, navigating the complicated landscape of safeguarding information and privacy regulations poses numerous difficulties. This section explores the main regulatory obstacles that stakeholders must overcome in order to comply with privacy regulations and put in place efficient compliance systems that reduce risks and guarantee accountability.

- Jurisdictional Diversity and International Reach: The digital landscape's jurisdictional complexity is one of the main obstacles to privacy legislation. When data is flowing freely across borders, it might be challenging to determine the appropriate legal framework and regulatory agency. Conflicting laws and disparate regulatory approaches exacerbate the issue, particularly when computing operations occur across multiple jurisdictions. The extraterritorial reach of some regulations, like the GDPR's application to companies outside the EU, further complicates matters by requiring enterprises to follow international rules or face incurring serious penalties and fines.
- Changing Technological Landscape and Regulation Lag: Authorities' capacity to create and implement pertinent rules and standards is frequently surpassed by the speed at which technological innovation is occurring. Because they generate enormous volumes of data and generate fresh dangers for data misuse and exploitation, Novel security and confidentiality risks are presented by cutting-edge technologies like blockchain, AI, and machine learning. Regulators find it difficult to keep up with these developments, which results in regulatory lag and coverage gaps that expose people and businesses to privacy violations and regulatory scrutiny.
- Regulatory Burden and Capacity Limitations: Small and medium-sized businesses and entrepreneurs with tight budgets and staffing levels must devote a great deal of time, money, and experience to comply with privacy rules. Organizations of all sizes have a significant compliance burden due to the intricacy of regulatory requirements, as well as the demand for continuous monitoring and risk assessment. Furthermore, a lack of resources may make it more difficult for businesses to put strong data security measures in place and deal with data breaches, which raises the risk of non-compliance and reputational harm.
- Data Security and Requirements for Notifying Breach: Protecting one's privacy and adhering to data protection regulations depend heavily on the security of personal data.
- Data security is still a major problem, though, as firms are constantly at risk from insider threats, cyberattacks, and data breaches. Organizations are required to swiftly notify affected persons and regulatory

organizations of any breaches of privacy that endanger their rights and freedoms, which adds another degree of complexity to compliance with breaches notification duties. Serious penalties and harm to the organization's reputation may follow noncompliance with these duties.

- Enforcing privacy rules effectively is crucial to discouraging noncompliance and making offenders answerable for their acts. Nevertheless, regulatory enforcement practices differ greatly between jurisdictions, with some authorities lacking the means or power to carry out exhaustive investigations and apply significant penalties. Additionally, the worldwide scope of data processing operations makes enforcement more difficult because, in order to effectively address cross-border violations, regulators must work with their colleagues in other jurisdictions. Building confidence in the regulatory structure and encouraging adherence to privacy regulations require bolstering regulatory enforcement and accountability systems. In conclusion, both companies and regulators face substantial obstacles due to privacy and data protection regulations. A complex strategy including stakeholder participation, technical advancements, and legislative reforms is needed to address these issues.

Data Defence in India and Abroad

In order to guarantee private information with regard to its integration, distribution, and other uses, nations all over the world have progressively built regulatory frameworks that cover almost every area. By examining how other nations throughout the world handle data protection, one can analyze India's strategy. There are several conventions pertaining to data protection, the most important of which being the 1980 rules established by the Organization for Development and Economic Cooperation. “OECD guidelines were framed with the motive to harmonise privacy norms among its members and to adhere free flow of data while complying with privacy norms. The OECD guidelines have affects data protection norms around the world but however these guidelines were updated in 2013 as much of it were found incompetent as time passed since its incorporation, but they are still found incompetent to deal with new issues arising out of data privacy and big data analytics”.

“Currently the two different models around the world for data protection is the European Union model and the American model, the American model provides a sector specific model whereas the European models and others adhering to it provides for a total right based approach provided comprehensively to the citizens. This shows the distinctiveness in the conceptual understanding of privacy in the two approaches”

European Perfect

The European model of data protection recognizes both the fundamental right to solitude and the liberty to protect information, as the main objective of data protection is to guarantee that information is appropriately shared throughout the union. To provide thorough protection against the transmission of data, the union thus complies with all of the OECD's specified criteria. One of the most important laws pertaining to data protection in the world is the General Data Protection Regulation of the EU of 2016, or EU (GDPR). The guidelines for data protection were updated in 2016 as the concept of data security and confidentiality norms continued to evolve alongside technological advancements norms. The regulation contains a number of rights, such as the ability to access, verify, ratify, modify, and so on. The European models suggests an independent supervisor with a variety of powers and responsibilities whose goal is to oversee data protection laws and ensure that people's important right to secrecy is respected. The supervisor also has the capacity to impose penalties.

Although European law has drawbacks of its own, including exceptions for national and social defense, etc., it is also quite successful and is adhered to by nations like Canada and Australia.

American Perfect

The fundamental tenet of the US's data protection legislation is laissez faire, or without intervention from the government. Instead of a single act that may be alluded to as a technology protection law, the United States has a number of sector-specific regulators that are limited in their operations to the individual sectors themselves. Despite the fact that the right to privacy is not expressly mentioned in the US Constitution, US courts have interpreted the Fourth Amendment's prohibition on search and seizure as relating to the privacy of personal information and secure.

Individual privacy in the public and private sectors are distinct in the United States. Public sector regulations, such the Privacy Act of 1974, are quite explicit. While the private sector is governed by sector-specific regulations like the Federal Trade Commission Act and the Children's Online Privacy Protection Act, this is based on FIPPS (the federal government's legislation managing data conditions) and other acts. Finally, the US approach is based on the notice and consent formula. Notice must be given before utilizing personal data, and no personal data may be used without permission.

Indian Perfect

India is trailing behind other nations, whether they are developed or developing. Even though the digital age has reached India as well, the Indian government recently unveiled the Digital India Initiative, a highly ambitious plan to connect the nation to the internet, which will automatically open up fresh business possibilities and generate income for the nation. The initiative aims to provide internet access to all of India's distinct settlements.

In the 2012 Puttaswamy case, the Supreme Court declared that the right to privacy is a fundamental one. Given that government action was now required to enact new regulations to safeguard people's privacy from both public and private institutions, such as the IT Act of 2000, this led to the establishment of new privacy standards in India. The Information Technology Act of 2019 (also known as the Information Rules or Reasonableness Security Practices and Sensitive Unique Material)

According to Section 43A of the IT Act, if a body corporate that operates, handles, or collects personal data about individuals fails to maintain a reasonable level of security for the data and a person suffers reasonable losses as a result, the body corporate will be required to pay compensation to the person or people impacted. Furthermore, Sections 72 and 72A discuss a person's criminal liability solely in the event that he reveals particulars without his consent during a transaction and he is harmed as a result. Therefore, these were the only laws that protected data privacy, and they were clearly ineffective.

Nonetheless, it is clear that strict data privacy regulations must be put in place by the government to ensure the success of the Digital India initiative. The government has even taken the necessary steps by forming the Srikrishna committee, which has promoted specific laws and even found a draft bill called the Personal Data Protection Bill, 2019; yet, the bill is presently on hold in the Indian Parliament due to a number of debates about its implications. Because the existing law is ineffectual in both its execution and its global ramifications, this situation must be changed immediately.

4. JUDICIAL AND LAW-MAKING GROWTHS ON RIGHT TO PRIVACY

Law-Making Developments

The Puttaswamy ruling in (Retd.) K. S. Puttaswamy v. The right to privacy was created by the Union of India as a basic freedom. Unquestionably, this case marked a turning point in the preservation of individual privacy; however, India had previously tried to safeguard information security through legislation, primarily through Article 21 of the structure, followed by the Information Technology Act of 2000 and other sector-specific laws, but these efforts ultimately proved unsuccessful..

In accordance with the OECD guidelines, which were enacted primarily to hold corporate entities accountable for rewards when they deal with, operate, handle, or collect personal data belonging to individuals and to require them to use appropriate security measures, the Technology (Reasonable Safety Practices and Sensitive Data or Info) regulations 2011 were created under Section 43A of the IT Act. However, it does not apply to companies that are owned by the government.

Furthermore, the government was mandated by the Aadhaar Act (Aadhar) to collect personal data about individuals, such as fingerprints, address, cellphone number, photograph, and more. The Unique ID Authority of India (UIDAI) was established to oversee the Aadhaar Act. The UIDAI needs to be completely secure in order to protect the privacy of the collected data. To this end, the Aadhaar System (Data Security) Statutes 2016 were created, requiring UIDAI to have all necessary security measures. However, despite this, the Aadhaar case and its associated controversy are well known, and there is no assurance that the data will be safe.

The RBI introduced the Credit Information Companies Act of 2005, another sector-specific law intended to protect individual privacy. Additionally, the Know the Customer rules restrict the information that bankers and other financial providers can request from their customers and hold them responsible for safeguarding that data.

“The same way the telecom sectors had the Telegraph Act and the TRAI Act, in it the telecom service providers are directed to take necessary steps to protect the privacy of its users by virtue of the service provided. And in the health sector in The Clinical Establishments (Central Governments) Rule 2012 requires to maintain the health information of individuals in an electronic format which is also a sensitive personal information as per the SPDI rules also the doctor patient relationship also should be maintained as per the Indian Medical Council (Professional Conduct Etiquette and Ethics) Regulation 2002”.

Judicial Growths

The judiciary's role in protecting people's privacy and recognising it as a basic right cannot be ignored. Prior to the right to private being recognised as a fundamental right, a number of decisions that described the right in the Putt case were made.

Firstly in M.P. Sharma case "the Supreme Court refused from recognising right to privacy as a constitutional or fundamental right and held that the power of search and seizure by a warrant as mentioned in section 94 and 96 of The Code of Criminal Procedure was not in contravention of any constitutional right and it is a necessary tool for the state to maintain rule of law in the country".

The second case involved Kharaksingh, and in this instance as too, the "Supreme Court observed that Article 21 of the constitution doesn't directly or expressly provide for a right to Privacy as a fundamental right even the question here raised that whether to maintain a surveillance state regular visits of officials even at night to the accused or blamed would be in contravention to the Right to Privacy. However Justice Subbha Rao held a dissending opinion and held privacy as an important facet relating to right to life and personal liberty".

Then in the circumstance of "Govind v. s of M.P this case was considered to be a positive development towards right to privacy as the court held that the word personal in Article 21 of the constitution holds spirit of privacy in it and it needs to be developed through case to case basis and also said that the right will not be absolute in nature. Here also the case was against the domiciliary visit of police to an accused at any time whether it being day or night".

Then, in the matter of R. Rajagopal and Anr. State of Tamil Nadu, it was decided that "right to privacy is inferred under right to life and personal liberty under Article 21 of the constitution. A resident has a privilege to shield the security of his own, his family, marriage, reproduction, parenthood, youngster bearing and instruction among different issues. None can distribute anything concerning the above issues without his assent regardless of whether honest or something else and whether commendatory or basic. In the event that he does as such, he would abuse the privilege to protection of the individual concerned and would be at risk in an activity for harms. Position may, notwithstanding, be unique, if an individual wilfully pushes himself into discussion or intentionally welcomes or raises a controversy".

In People's Union of Civil Liberties (PUCL) v. Union of India, the Supreme Court came to the unmistakable conclusion that the right to privacy is a fundamental component of the constitutionally protected rights to freedom and the pursuit of choice in Article 21 and that these rights can only be restricted through legally mandated processes.

Last but not least, the Puttaswamy ruling, sometimes referred to as the Aadhaar case, was a major decision in the privacy domain, "the question in the case was whether the collection of personal data for the purpose of Aadhaar card such as biometrics, photo, signature etc. would be the breach of privacy under Article 21 of the constitution in it constitutional bench comprising of 9 judges held that right to privacy is in integral part of Article 21 of the constitution and privacy is availed at the world at large and against the state as well however it's not absolute and right to privacy can be taken away by a just fair and a reasonable established method by law".

Because of this ruling, the government is now required to enact new laws to safeguard individual privacy.

Intelligences on Data Protection

The operational Planning Commission at the time established the A.P. Shah Committee, which is led by Justice A.P. Shah, to conduct a thorough analysis of India's privacy laws. Authorities primarily established two committees—the A.P. Shah Committee and the Srikrishna Committee Report—to address the issue of data violation. The 2018 Private Data Protection Bill was a draft bill that the latter even submitted on the subject. It serves as the foundation for India's privacy laws. The committee is credited with establishing India's privacy regime because it served as the first protection-related initiative of any kind in the nation. It outlines nine guidelines for data protection across the country and is primarily based on OECD standards.

The Supreme Court's Puttaswamy decision led to the creation of the Srikrishna Committee in July 2017. The measure controlling the protection of individual data, which attempts to safeguard people's personal information while encouraging the development of the virtual economy, has been well-presented by the panel. The legislative branch is still considering the bill. "According to this committee the data protection is the base and the foundation on which innovation and entrepreneurship ca prosper in India moreover in this globalising world where mostly all the developed or developing countries in the world have some or the other methods of data protection it was high time that India also implements the same. This committee also proposed that for a better technological and digital future and for the fulfilment of digital India initiative data protection laws are a must".

This committee carefully reviews all data protection laws across the globe, including international recommendations, in order to develop effective and efficient privacy legislation for the country. To get public

input on a variety of issues, such as the extent of data safeguards and exceptions, the committee even produced a white paper.

But the draft measure is still waiting, and the government has even suggested numerous exceptions based on national interest and public policy, which President Srikrishana himself is criticizing.

5. CONCLUSION AND SUGGESSIONS

Given that other countries, whether in Europe, America, Australia, or China, have already implemented data protection legislation, the aforementioned research makes it clear that India urgently needs them. However, despite judicial action on the matter, the nation's current laws—especially the IT Act—are inadequate to handle data privacy issues affecting the government or commercial organisations. The government's Digital India project established the Srikrishna committee to draft a data management legislation and provide detailed recommendations on its founding principles because the Puttaswamy verdict highlights the tight relationship between data protection and privacy.

The problem with that of internet is that if anything is uploaded there on the internet, then it’s very difficult to remove it or even stop it from circulating thus it must be stopped from the very beginning from its origin itself thus as said above immediate and The nation needs to enact data protection laws effectively. Although the measure has not yet been ratified by Parliament, it is certain that private organizations will not be allowed to utilize personal information without any limitations; however it is yet unclear what those limitations will be for the authorities. It is safe to state that anonymity law that will impact the existence of every internet user is about to be implemented. To have an immediate impact on the ground level, privacy changes must be accompanied with increases in state culpability.

REFERENCES

[1] Shahid, J., Ahmad, R., Kiani, A. K., Ahmad, T., Saeed, S., & Almuhaideb, A. M. (2022). Data protection and privacy of the internet of healthcare things (IoHTs). Applied Sciences, 12(4), 1927.
[2] Hallinan, D., De Hert, P., & Leenes, R. (2021). Data Protection and Privacy.
[3] Hartzog, W., & Richards, N. (2020). Privacy's constitutional moment and the limits of data protection. BCL Rev., 61, 1687.
[4] Babikian, J. (2023). Securing Rights: Legal Frameworks for Privacy and Data Protection in the Digital Era. Law Research Journal, 1(2), 91-101.
[5] Shahrullah, R. S., Park, J., & Irwansyah, I. (2024). Examining personal data protection law of Indonesia and South Korea: The privacy rights fulfilment. Hasanuddin Law Review, 10(1), 1-20.
[6] ThankGod Chinonso, E. (2023). The impact of chatgpt on privacy and data protection laws. The Impact of ChatGPT on Privacy and Data Protection Laws (April 16, 2023).
[7] Sarabdeen, J., Chikhaoui, E., & Ishak, M. M. M. (2022). Creating standards for Canadian health data protection during health emergency–An analysis of privacy regulations and laws. Heliyon, 8(5).
[8] Brauneck, A., Schmalhorst, L., Kazemi Majdabadi, M. M., Bakhtiari, M., Völker, U., Baumbach, J., ... & Buchholtz, G. (2023). Federated machine learning, privacy-enhancing technologies, and data protection laws in medical research: scoping review. Journal of medical Internet research, 25, e41588.
[9] Choe, J. Y., Son, D., & Kim, S. (2017). The Limitations on the Use of Big Data Pursuant to Data Privacy Regulations in Korea. J. Korean L., 17, 1.
[10] Christou, G., & Lee, J. S. (2022). EU-South Korea Cooperation on Cybersecurity, Data Protection and Emerging Technologies. Cybersecurity Policy in the EU and South Korea from Consultation to Action: Theoretical and Comparative Perspectives, 41-66.
[11] Kim, D. H., & Park, D. H. (2024). Automated decision-making in South Korea: a critical review of the revised Personal Information Protection Act. Humanities and Social Sciences Communications, 11(1), 1-11.
[12] Jeon, S. J., Go, M. S., & Namgung, J. H. (2023). Use of personal information for artificial intelligence learning data under the Personal Information Protection Act: the case of Lee-Luda, an artificial-intelligence chatbot in South Korea. Asia Pacific Law Review, 31(1), 55-72.
[13] ZHANG, G., & JIANG, J. (2022). A Comparative Study of Consent Rules in the Personal Information Protection Laws of China and South Korea. 국제거래와 법, (39), 1-34.
[14] Bygrave, L. A. (2010). Privacy and data protection in an international perspective. Scandinavian studies in law, 56(8), 165-200.
[15] Kim, E. C., Kim, E. Y., Lee, H. C., & Yoo, B. J. (2021). The details and outlook of three data acts amendment in south korea: with a focus on the changes of domestic financial and data industry. Informatization Policy, 28(3), 49-72.
[16] Ko, H., & Park, S. (2020). How to de-identify personal data in South Korea: an evolutionary tale. International Data Privacy Law, 10(4), 385-394.
[17] Lee, S. G., & Kim, E. (2022). Self-Quarantine System and personal information privacy in South Korea. Yonsei medical journal, 63(9), 806.

[18] Lee, Y., & Jung, I. Y. (2021). Identifying stakeholder perspectives on data industry regulation in South Korea. Journal of Information Science Theory and Practice, 9(3), 14-30.
[19] Shin, Y. J. (2021). The improvement plan for personal information protection for artificial intelligence (AI) service in South Korea. Journal of Convergence for Information Technology, 11(3), 20-33.
[20] Park, S., Choi, G. J., & Ko, H. (2020). Information technology–based tracing strategy in response to COVID-19 in South Korea—privacy controversies. Jama, 323(21), 2129-2130.
[21] Gillispie, C. (2021). How Can South Korea Teach, Lead, and Better Engage with the Asia-Pacific in Shaping Data Governance for the 5G Era?. asia policy, 16(4), 143-166.
[22] Jung, C. Y., & Joo, H. K. (2023). Post-'Lee-Luda'personal information protection in Korea: developer responsibility and autonomous AI governance. International Data Privacy Law, 13(2), 154-167.
[23] Banisar, D., & Davies, S. (1999). Global trends in privacy protection: An international survey of privacy, data protection, and surveillance laws and developments. J. Marshall J. Computer & Info. L., 18, 1.
[24] Lee, J. H., Suh, J., & Roh, J. (2021). Current Status and Issues in Digital Trade Agreements: Focusing on Cross-Border Data Flows and Data Protection. Korea Trade Review, 46(3), 99-117.
[25] Yoon, S. P., Joo, M. H., & Kwon, H. Y. (2019). How to guarantee the right to use PSI in the age of open data: Lessons from the data policy of South Korea. Information Polity, 24(2), 131-146.