Page 184 - 207 **DOI:** *https://doij.org/10.10000/IJLMH.116092*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 6 | Issue 6

2023

Understanding India's New Data Protection Laws and their Influence on the Constitutional Right to Privacy

KHUSHI PRADEEP RINWA[1]

ABSTRACT

An internationally recognized fundamental human right is privacy. However, in the era of digital technology, safeguarding personal data faces significant hurdles. This research paper provides a detailed exploration of the evolution of privacy rights in India, underscoring the critical role of data protection legislation. The paper begins by illuminating the urgency of addressing privacy concerns in the digital age, emphasizing the ethical handling of data, the protection of user rights, prevention against misuse, and the overall safeguarding of individuals' interests. It considers the complicated world of digital data while looking into historical background and the requirement for data protection laws in India. It also emphasizes necessity in establishing comprehensive legal frameworks to regulate these practices effectively. It also covers the evolution of digital personal data protection laws in India and how data protection laws have changed over time. Moreover, the paper highlights the basic requirement for thorough information assurance regulations in India to guarantee information security and protection in an undeniably computerized world. It calls for swift legislative action to tackle evolving digital technology challenges and advocates for transparency, fairness, and accountability in data collection and processing practices.

Keywords: *Privacy, Human right, Personal Data, Data Protection Law, Data Security, necessity.*

I. INTRODUCTION

Privacy is the concept that individuals or groups should have the ability to keep their personal information hidden from others and maintain their personal space. This concept is regarded as a basic human right and is enshrined in international agreements like Article12 of the Universal Declaration of Human Rights (UDHR).

Article12 emphasizes the Right of every Individuals should have the freedom to be exempt from interference. with their privacy, including their personal correspondence, family matters, and

[1] Author is a student at University of Mumbai, Thakur Ramnarayan College of Law, Mumbai, Maharashtra, India.

 [ISSN 2581-5369]

reputation. It also highlights that individuals have the entitlement to protection against such intrusions.[2]

The notion of privacy has deep historical roots and is regarded as an inherent part of human rights from the moment of birth. These rights encompass various aspects, including the right to solitude, the confidentiality of communication, bodily privacy, and safeguarding personal information.[3] However, it's important to note that these rights do not extend to private information that serves an information accessible in the form of public records in the interest of the public.

Privacy is essential for leading a dignified life. Our society witnesses various forms of cybercrime activities such as phishing, viruses, ransomware, hacking, and spamming. To mitigate these risks and protect individuals' personal information, there is a strong requirement for stringent Data Protection Laws.

Data Protection Laws constitute a comprehensive combination of regulations, procedures, and policies aimed at reducing infringements on Privacy of individuals compromised through The handling, gathering, and dissemination of personal information or data, in this context, pertain to details that enable the identification of an individual, regardless of whether it is acquired by an organization or a government entity.

Citizens and consumers need the tools necessary To assert their entitlement to privacy and safeguard both themselves and their data against improper utilization. Data protection is a critical component of preserving our fundamental Right to Privacy, which is upheld by worldwide and provincial regulations and settlements. It involves legal framework established to safeguard one's Personal data which is collected, processed, and stored through strategies or expected for consideration in a documenting framework.[4]

It is imperative that data protection laws regulate and influence the actions of corporations as well as government. These regulations grant individuals the authority protect the data from potential exploitation. Without such regulations, institutions have demonstrated a tendency to accumulate, analyse, and retain all data while disclosing very little to the individuals concerned.

---

[2]Jayanta Boruah & Bandita Das, Right to privacy and data protection under Indian legal regime SSRN (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3827766#:~:text=Privacy%20has%20emerged%20as%20a, become%20very%20difficult%20to%20achieve.

[3] Sumedha Ganjoo, Right to privacy and data protection laws in India balancing rights and managing conflicts Shodhganga@INFLIBNET: Right to Privacy and Data Protection Laws in India Balancing Rights and Managing Conflicts (1970), https://shodhganga.inflibnet.ac.in:8443/jspui/handle/10603/440613?mode=full

[4]Vijay Pal Dalmia, Data Protection Laws in India - everything you must know - data protection - india Data Protection Laws In India - Everything You Must Know - Data Protection - India (2017), https://www.mondaq.com/india/data-protection/655034/data-protection-laws-in-india---everything-you-must-know

 [ISSN 2581-5369]

Data protection laws are crucial for safeguarding privacy and ensuring individuals have control over their personal information in today's technology-driven world.

II. GROWTH OF RIGHT TO PRIVACY IN INDIA AS FUNDAMENTAL RIGHT IN INDIA

The following significant court rulings have contributed to the evolution of the right to privacy basic right in India:

- In the case of MP Sharma vs. Satish Chandra (1954) an issue raised was whether or not the right to privacy was violated by search and seizure authorities. Nevertheless, the court determined that the architects of the Indian Constitution did not have the intention of incorporating the right to privacy as a fundamental right in its stipulations. This decision was a significant setback for privacy advocates at the time, as it did not establish privacy as a fundamental right.[5]
- The case of Kharak Singh vs. The State of UP (1964) Kharak Singh challenged the surveillance carried out under Uttar Pradesh regulations, particularly nighttime surveillance, which was seen as a violation of personal liberty and an intrusion into one's home. The Supreme Court ruled against Regulation 236(b) but did indirectly recognize privacy as a fundamental right. Hence, it's crucial to remember that Justice SubhaRao held a differing opinion, asserting that privacy is an inherent aspect of Article 21, even if not explicitly recognized.[6]
- The case of Govind vs State of Madhya Pradesh (1975) also challenged police surveillance regulations. The Supreme Court did not strike down these regulations but emphasized that privacy rights could be Subject to rational limitations in the pursuit of public safety.. This decision reinforced the idea that privacy rights were not absolute and could be limited under certain circumstances.[7]
- In the case of Malak Singh vs state of Punjab & Haryana & Others(1981)clarified that state surveillance conducted within the boundaries of the law and without infringing on personal liberty is lawful. It underscored the importance of adhering to established legal procedures when conducting surveillance.[8]

[5] M. P. Sharma and others vs Satish Chandra, district on 15 March, 1954, https://indiankanoon.org/doc/1306519/
[6] Kharak Singh vs the state of U. P. & others on 18 December, 1962, https://indiankanoon.org/doc/619152/
[7] Govind vs state of Madhya Pradesh & ANR on 18 March, 1975 https://indiankanoon.org/doc/436241/
[8] Malak Singh Etc v. State of Punjab & Haryana &others on 5 December 1980 https://indiankanoon.org/doc/971635/

 [ISSN 2581-5369]

- In the case of R. Rajagopalan vs. State of Tamil Nadu(1994) marked a very important turning point in recognising the privacy rights. As indicated by the Supreme court , Article 21 inherent the right to privacy, highlighting Every Indian citizen possesses the freedom to protect their privacy. It particularly emphasized matters related to education, child-rearing, reproduction, marriage, and family as protected aspects of privacy.[9]
- In the case of People's Union for Civil Liberty vs UOI (1996) challenged the constitutional validity of telephone tapping.[10]Supreme Court ruled that a telephone conversations are an essential aspect in a person's life and tapping them without proper legal.

The violation of privacy rights under Article 21 is evident in these procedures. Nevertheless, it observed that the state. Surveillance could be allowed if there was a law specifying the procedure or if it adhered to rules framed under the Telegraph Act.

The culmination of these cases led to a significant development in the recognition of privacy rights in India. While privacy was not expressly established as a fundamental right in the preceding.

Cases like Kharak Singh and MP Sharma, it was finally established as such in the 2012 Puttaswamy case. In this case, the Supreme court clearly and officially upheld the fundamental nature of the right to privacy in this case. ensured under third part of the Constitution, specifically within Article 21[11].

Hence, the journey to recognizing privacy as a fundamental right in India involved a series of judicial decisions that gradually expanded the scope and importance of privacy rights, culminating in the landmark Puttaswamy case where privacy was explicitly declared as a fundamental right. This evolution underscores the significance of privacy in the context of individual liberties and constitutional rights in India.[12]

III. NECESSITY OF DATA PROTECTION LAWS

Privacy and data protection serve several essential purposes. Firstly, privacy is crucial for our personal safety, as the public availability of our personal information can potentially expose us

[9] R. Rajagopal vs state of T.N on 7 October, 1994 https://indiankanoon.org/doc/501107/
[10] People's Union of Civil Liberties ... vs Union of India (UOI) and ANR ..., https://indiankanoon.org/doc/31276692/
[11]Justice K.S.Puttaswamy(Retd) vs Union of India on 26 September, 2018, https://indiankanoon.org/doc/127517806/
[12] People's Union of Civil Liberties ... vs Union of India (UOI) and ANR ..., https://indiankanoon.org/doc/31276692/

 [ISSN 2581-5369]

to harm. Secondly, privacy is fundamental for preserving our personal freedom[13], as the widespread disclosure of personal data can be exploited to exert control over individuals. For instance, if an employer has access to one's address, it becomes easier to send work-related materials without consent.

Preserving our personal dignity is essential and privacy plays a vital role in this, as publicly accessible private information can be exploited to subject individuals to humiliation. Additionally, it plays a vital role in protecting our personal relationships, as divulging personal data can be used to harm these connections.[14] Moreover, privacy is integral to maintaining our personal identity since the unauthorized use of publicly available personal information can lead to impersonation.

Data protection legislation stands as a cornerstone of our digital society, providing a comprehensive framework to ensure that private information is treated with the utmost care and ethical responsibility. These laws exert control over every aspect of personal data, encompassing its collection, utilization, transmission, and disclosure, as well as the security measures necessary to shield it from unauthorized access[15]. By doing so, they uphold the fundamental principles of data privacy, safeguarding individuals against the myriad risks that stem from the mishandling of their personal information.

Granting individuals, the right to access their own data is a key objective of data protection laws. This transparency empowers people to have greater control over their personal information, allowing them to inquire about and retrieve data held by organizations, thus promoting a culture of openness and accountability. Moreover, these laws establish clear accountability standards for businesses and entities that process personal data. This accountability ensures that organizations handle such information with care and in compliance with established guidelines, fostering trust among data subjects and the public at large. In the event that personal data is processed improperly or harmfully, individuals have recourse options thanks to data protection laws. This includes addressing instances of data breaches, unauthorized use, or other forms of data mishandling, thereby providing individuals with recourse when their data is compromised.

[13]Right to privacy and Data Protection Era, Legal Service India - Law, Lawyers and Legal Resources, https://www.legalserviceindia.com/legal/article-10664-right-to-privacy-and-data-protection-era.html

[14]Jayanta Boruah & Bandita Das, Right to privacy and data protection under Indian legal regime SSRN (2021),https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3827766#:~:text=Privacy%20has%20emerged%20as%20a,become%20very%20difficult%20to%20achieve.

[15] Data Protection Laws in India, Data Protection in India- India Law Offices, https://www.indialawoffices.com/legal-articles/data-protection-laws-in-india

Additionally, data protection laws address the alarming issue of false profiles and fraudulent activities perpetrated using stolen personal information. By doing so, they aim to combat various forms of cybercrime, identity theft, and online fraud that can harm individuals and organizations alike. The significance of data protection laws cannot be overstated. Negative effects may arise if personal information is obtained by unauthorized individuals., affecting individuals' safety and well-being on multiple levels. This includes economic security, as stolen data can be exploited for financial gain, as well as physical safety, given the potential for harassment or harm resulting from unauthorized access to personal information.[16]

Furthermore, breaches of data privacy can compromise an individual's personal integrity and reputation. Data protection laws serve as a safeguard to protect users from exploitation and the unauthorized use of their personal information. They ensure responsible data handling, promote trust in our digital society, and safeguard the rights and security of individuals, recognizing the pivotal role that data privacy plays in the modern world.

IV. EFFORTS MADE FOR DATA PROTECTION IN INDIA

In response to the rising challenges of data theft and breaches of data privacy in India, To strengthen data protection measures, a number of noteworthy efforts have been made. The government, along with various industries, has recognized the need to go beyond the existing legal framework to address these issues. One significant effort includes the proposed amendments (IT) Act of 2000 by the Ministry of Communications and Information Technology. These proposed amendments led to the IT (Amendment) Act of 2008[17], introducing pivotal provisions such as Section 43A, emphasizing the importance of implementing reasonable security practices for the protection of sensitive data and Section 72A addresses the information disclosure in violation of legal contracts. However, it's important to note that these proposed amendments are yet to be fully incorporated into the existing Act, resulting in the establishment of new regulations known as the Privacy Rule.

The Privacy Rule, introduced subsequently by the ministry of Communication and information technology, aims to bridge the gap between the proposed amendments and their actual implementation. It places significant emphasis on the importance of adopting reasonable security practices when handling sensitive personal data and highlights the potential sanctions for noncompliance under Section 43A. Notably, this rule does not specify specific limits for

[16] Sneha Mahawar, Data Protection Laws in India iPleaders (2023), https://blog.ipleaders.in/data-protection-laws-in-india-2/

[17]Eprocure.gov.in, https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMTk4NzY=

 [ISSN 2581-5369]

compensation in the event of non-compliance, leaving some room for interpretation.[18]

Moreover, the Privacy Rule exclusively addresses Sensitive Personal Data or Information (SPD), providing a comprehensive definition of this category, which includes highly sensitive data such as credit/debit card information, biometric data, and health-related information. The rule also offers clarity by stating that publicly available data that can be accessed without cost is not considered SPD.

Another crucial aspect of these developments is the responsibilities imposed on "body corporates" and other entities responsible for handling sensitive data.[19] These organizations are obligated to implement rational security procedures to protect the data they manage. Importantly, the Privacy Rule allows individuals to seek compensation for any harm resulting from information violations.

To further support and guide these efforts, the information Security Council of India, established by NASSCOM, serves as a self- regulatory body dedicated to developing data privacy and security standards within the industry, thereby offering a platform for the exchange of knowledge and expertise in the domain of data security. Additionally, to address concerns regarding unsolicited calls and telephone number privacy, the telecom regulatory authority of india(TRAI) has implemented the National Do Not Call Registers, empowering subscribers to block unwanted calls and better safeguard their privacy. In light of the quickly advancing computerized scene, these actions highlight India's proactive way to deal with shielding information in a period set apart by expanded web-based exercises and interconnectedness. They safeguard individual security as well as encourage a climate helpful for advancement and computerized trust, which is fundamental for the nation's monetary and innovative development. As India keeps on adjusting to the computerized age, these aggregate estimates expect to work out some kind of harmony between information driven progress and the basic of safeguarding residents' very own data.

V. PRIVACY LAWS IN OTHER COUNTRIES

(A) Privacy Laws in the United Kingdom

The originator of the common law system in the United Kingdom has been making efforts to develop laws on privacy since 1948. During that period, there were no specific laws addressing privacy concerns, and the handling of privacy violations relied on the concept of a breach of

[18] Right to privacy and Data Protection Era, Legal Service India - Law, Lawyers and Legal Resources, https://www.legalserviceindia.com/legal/article-10664-right-to-privacy-and-data-protection-era.html
[19] ibid

confidence. Initially, privacy was primarily considered as a breach of confidence before gaining recognition as a breach of human rights through pivotal cases like Von Hannover v. Germany (2005)[20] and PG and JH v. United Kingdom (2001).[21] These cases underscored the importance of privacy, leading to the understanding of how important it is to safeguard and honour a person's privacy.

In response to these developments, The United Kingdom passed the Human Rights Act in 1998 to align its legal framework with the European Convention on Human Rights. Nevertheless, when we compare privacy laws between the United States and the United Kingdom, it becomes evident that the UK's privacy laws are not as advanced or comprehensive.

The United States enacted its Privacy Act in 1974, while the United Kingdom's first legislation for protecting individuals' privacy consisted of the Human Rights Act 1998 and the Data Protection Act 1998. Presently, the UK has introduced some statutory provisions aimed at safeguarding the right to privacy. These provisions have taken the form of Parliamentary initiatives, constitutional reports, and statutory enactments.

The key elements of these privacy laws and initiatives are as follows:

a) Recognition of privacy as a tort under Civil Law.

b) The application of the Law of Trust or Confidence.

c) The Wireless Telegraphy Act of 2006.

d) Provisions within the Theft Act of 1968.

e) The introduction of Private Members' Bills between 1961 and 1970.

f) Findings and recommendations from the Younger Committee Report in 1972.

g) The Rehabilitation of Offenders Act in 1974.

The British legal system operates within an uncodified constitution, making it challenging to identify privacy as a constitutional right in the UK. This unwritten constitution draws from various sources, including Acts of Parliament, court rulings, and established conventions. Key sources that contribute to the legal framework include the Bill of Rights, the European Convention on Human Rights, Fundamental Freedom 1950 and the Human Rights Act of 1998.

[20] Akshhatha Adarssh, A comparative study of right to privacy as a human right with special reference to India United Kingdom and USA Shodhganga@INFLIBNET: A Comparative Study Of Right To Privacy As A Human Right With Special Reference To India United Kingdom And USA (1970), https://shodhganga.inflibnet.ac.in:8443/jspui/handle/10603/454832 (last visited Nov 1, 2023).

[21] Sumedha Ganjoo, Right to privacy and data protection laws in India balancing rights and managing conflicts Shodhganga@INFLIBNET: Right to Privacy and Data Protection Laws in India Balancing Rights and Managing Conflicts (1970), https://shodhganga.inflibnet.ac.in:8443/jspui/handle/10603/440613?mode=full

Although privacy law in the UK has evolved substantially, it is distinct in that it is not rooted in a predefined legal text but instead relies on a dynamic system of judicial decisions. This flexibility enables the law to adapt and expand its interpretation of privacy in accordance with changing societal norms and circumstances.

(B) Privacy Laws in the USA

The recognition of the right to privacy in US began with the 1965 case of Griswold v. Connecticut,[22] which marked a significant turning point. Prior to this case, the Harvard Law Review, authorized by Warren and Brandeis[23], published an article defining privacy as the "right to be left alone." Subsequently, The Apex Court expanded the right to privacy in the case of Eisenstadt, where it discussed the right of unmarried couples to purchase contraceptives, emphasizing that this right belonged to the individual, not just married couples.

The Supreme Court additionally took inspiration for the idea of the right to privacy from the Fourteenth Amendment in case of Roe, [24]extending it to incorporate a woman's right of abortion. The Fourteenth Amendment's definition of personal liberty and its limitations on state action were found to protect a woman's right to terminate her pregnancy. The 14th Amendment's Due Process Clause was invoked in the Lawrence case. was used to further expand this idea by granting privacy protections to people of the same sex engaging in consensual sexual conduct.[25]

The right to privacy is entrenched by amendments of the United States Constitution, even though it is not protected outright. While the First and Fifth Amendments primarily safeguard individual autonomy, the Fourth Amendment forbids arbitrary searches and seizures.

The Privacy Act of 1974 forbids government agencies from revealing personally identifiable information to third parties and ensures that individuals have access to certain government records pertaining to themselves. Tort law serves as an effective mechanism to handle privacy violations, allowing individuals to seek injunctive relief or recover damages in cases of privacy violations driven by malice or motives of gain. It safeguards individuals against emotional disturbances and invasions of their privacy. The legal and constitutional framework in the

[22]Griswold v. Connecticut, 381 U.S. 479 (1965) (no date) Justia Law. Available at: https://supreme.justia.com/cases/federal/us/381/479/

[23]Akshhatha Adarssh, A comparative study of right to privacy as a human right with special reference to India United Kingdom and USA Shodhganga@INFLIBNET: A Comparative Study Of Right To Privacy As A Human Right With Special Reference To India United Kingdom And USA (1970), https://shodhganga.inflibnet.ac.in:8443/jspui/handle/10603/454832

[24] Sumedha Ganjoo, Right to privacy and data protection laws in India balancing rights and managing conflicts Shodhganga@INFLIBNET: Right to Privacy and Data Protection Laws in India Balancing Rights and Managing Conflicts (1970), https://shodhganga.inflibnet.ac.in:8443/jspui/handle/10603/440613?mode=full

[25] Sanctity of personal data: A Comparative Study of data privacy laws in ..., https://thelawbrigade.com/wp-content/uploads/2020/05/Anisha-IJLDAI.pdf

United States provides strong protections for privacy., as reflected in various federal and state privacy laws. These laws cover a wide range of sectors, including The Privacy Act of 1974 establishes guidelines for the gathering, utilizing, storing, and sharing of individually identifiable data. These guidelines are based on fair information practices.

Overall, the right to privacy is firmly established in the States, with a well-developed legal foundation, and is protected through both judicial decisions and legislative measures, making the country's legal system advanced and comprehensive in safeguarding privacy. This multi-layered approach demonstrates the nation's commitment to upholding personal freedoms and privacy rights.

VI. INITIATIVE TAKEN FOR DATA PROTECTION IN INDIA

India has taken various steps to bolster its data protection standards, augmenting its existing legal framework for data security. The Ministry of Information Technology Act in India has spearheaded few measures aimed at raising the bar for data security.

One of these initiatives is the establishment of the Standardization Testing and Quality Certification (STQC) Directorate, overseen by the government under the Department of Information Technology (DIT). The Head Office responds regarding the global demand for Indian businesses to meet international security standards.[26] The STQC Directorate also offers services like staff training in quality and security standards and procedures, as well as testing and certifying software and hardware products.

Furthermore, another critical component in India's data protection infrastructure is the Computer Emergency Response Team (CERT-In), also established by DIT. CERT-In plays a pivotal role in the global CERT community, with its primary mission being the safeguarding of IT resources in India are protected from viruses and security risks. It serves as a central point of contact for handling computer security incidents, disseminating best practices for system managers and service providers, raising knowledge and awareness about Computer security and information security concerns among Indian internet users issuing advisories and vulnerability notes to keep the community informed about the latest security threats, acting as a hub for organizations to collaborate on addressing computer security issues, establishing connections with similar international organizations, and engaging in research and development activities in collaboration with prominent research and educational institutions to tackle prevailing system

[26]Jayanta Boruah & Bandita Das, Right to privacy and data protection under Indian legal regime SSRN (2021),https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3827766#:~:text=Privacy%20has%20emerged%20as%20a,become%20very%20difficult%20to%20achieve.

security concerns and emerging cybersecurity challenges.[27] These measures reflect India's commitment to enhancing data protection and cybersecurity on both national and global fronts.

It is imperative to approach data collection and processing activities with transparency and equity as fundamental principles. Individuals should have a clear understanding of why their data is being collected and how it will be used. Additionally, comprehensive data protection measures must be in place throughout the entire lifecycle of data, covering collection, storage, and transmission. Data protection policies and procedures must be customized to each organization's unique needs and characteristics in order to be effective. Education and awareness among employees regarding data protection are essential. They need to grasp the significance of compliance with relevant laws and regulations. It is paramount that all collected data is shielded and processed In a way that upholds an individual's privacy rights. Emphasizing this data collection principle not only demonstrates ethical responsibility but also ensures compliance with data protection regulations, like GDPR and CCPA. Additionally, it minimizes the risk of data breaches and misuse, fostering a more secure digital environment. Overall, a conscientious approach to data collection aligns organizations with the evolving landscape of data privacy and establishes a foundation for responsible and sustainable data management practices.

(A) Right to Privacy Post Puttaswamy

The landmark Aadhaar judgment concerning privacy, A number of matters were taken into consideration, such as the Aadhaar Act's constitutionality. This matter is succinctly analysed as follows:

The Indian government launched the Aadhaar programme in 2009 with the goal of directly benefiting Indian citizens. In order to provide identity verification and facilitate access to government welfare programs like LPG distribution and the Jan Dhan Yojana, it established a distinct identifier, the Aadhar number which is of 12 digits. These digits were issued by the Unique Identification Authority of India (UIDAI), which was also responsible for gathering biometric data (fingerprints, iris scans, and other biometrics) and demographic data (name, address, and sex). The scheme in question faced several significant challenges. Firstly, there were concerns about its regulatory framework as it relied on executive orders rather than being formalized through an Act of Parliament, which raised questions about its legal standing and oversight.[28] Secondly, the data collection aspect of the scheme was entrusted to private

[27] Right to privacy and Data Protection Era, Legal Service India - Law, Lawyers and Legal Resources, https://www.legalserviceindia.com/legal/article-10664-right-to-privacy-and-data-protection-era.html

[28] Justice K.S.Puttaswamy(Retd) vs Union of India on 26 September, 2018,

 [ISSN 2581-5369]

agencies, and this led to worries about data security. There was a lack of adequate provisions to ensure the protection and privacy of the collected data. Thirdly, there were insufficient legal safeguards to prosecute individuals or entities that might misuse or fail to utilize the collected data for its intended purpose, which posed a risk of potential abuse and misuse of the gathered information. These issues brought about serious concerns and debates surrounding the scheme's implementation and effectiveness.

To address these concerns, the Aadhaar Bill was passed in 2016, subsequently becoming an Act, with the primary objective of providing legislative support to the Aadhar scheme[29]. After its enactment, various notifications were issued mandating the linking of Aadhaar with PAN, phone numbers, bank accounts, and other services.

Many petitions were filed in response to Aadhaar, mostly on the grounds of privacy infringement, contesting the system's constitutionality. Ashok Bhushan, Chief Justice Dipak Mishra, A.M. Khanwilkar, Justices A.K. Sikri and Dhananjaya Yeshwant Chandrachund made up the five-judge Supreme Court bench that heard these challenges. Finally, with a 4:1 majority vote, the Aadhaar Act was deemed constitutionally valid. However, certain provisions, including Section 57, Section 47, and Section 33(2), were struck down. Consequently, private entities can no longer request Aadhaar numbers, and individuals have the right to file complaints against entities and the government for rights violations. One of the judges, J. Chandrachud, dissented, arguing that the Act was unconstitutional as it undermined the Rajya Sabha and contravened the constitutional framework.[30]

The Supreme Court's decision on the Aadhaar Act led to significant reforms, strengthening individuals' rights and data protection. It also sparked a national dialogue on digital privacy and the changing relationship between technology and personal liberties in the modern era.

VII. CHALLENGE OF DIGITAL DATA PROTECTION

In the digital age, there has been a growing emphasis on the right to privacy, particularly as technological advancements facilitate the sharing of more personal information. Nonetheless, this right remains inadequately protected in India due to recent developments that pose threats to individual privacy. Companies like Facebook and Google have the capability to amass extensive data on individuals and employ it for targeted advertising without their explicit

https://indiankanoon.org/doc/127517806/

[29] The aadhaar (targeted delivery of financial and other subsidies ..., https://uidai.gov.in/images/Aadhaar_Act_2016_as_amended.pdf .

[30] Justice K.S.Puttaswamy(Retd) vs Union of India on 26 September, 2018, https://indiankanoon.org/doc/127517806/

 [ISSN 2581-5369]

consent or knowledge, raising concerns about the safeguarding of personal privacy as a fundamental right[31]. Additionally, the digital era has ushered in new complexities in terms of privacy and data security. Criminals and terrorists are exploiting technology for surveillance and espionage, and the proliferation of artificial intelligence and automation introduces challenges to individual privacy through automated decision-making processes that can infringe upon personal data. Addressing these issues necessitates collaborative efforts between governments and businesses to establish policies and regulations that strike a balance between technological progress and the protection of privacy.

While the digital age brings various advantages such as improved communication and collaboration, it concurrently gives rise to privacy concerns in India. The absence of a robust legal framework governing digital technologies exposes individuals to online abuse and exploitation. Concerns about user The widespread utilization of technology also gives rise to concerns regarding security and privacy. social media and mobile devices.

India needs to take action to protect its citizens' privacy and create comprehensive legal guidelines for the use of digital technology in order to address these issues. The country has lagged behind in keeping pace with technological advancements, resulting in numerous instances of companies violating data protection laws and experiencing data breaches with severe consequences for individuals and businesses. To ensure privacy protection and prevent data breaches, India should enhance its legislation related to data protection and bolster the mechanisms for its enforcement.

Managing the complexities of privacy and data protection within the digital landscape demands careful consideration. There are a few important steps that need to be considered when developing and putting into practice policies and procedures concerning these rights. Transparency and fairness are paramount, as they guarantee It is important that individuals are informed about the reason for data collection and its intended utilization. while also ensuring fairness in data practices[32]. Data lifecycle protection is vital, encompassing security measures and access controls at every stage of data handling. Tailored policies and procedures are essential, recognizing the unique needs of different organizations. Employee education is pivotal, as well-trained personnel can help prevent data breaches. Consistency with privacy

[31] Akshhatha Adarssh, A comparative study of right to privacy as a human right with special reference to India United Kingdom and USA Shodhganga@INFLIBNET: A Comparative Study Of Right To Privacy As A Human Right With Special Reference To India United Kingdom And USA (1970), https://shodhganga.inflibnet.ac.in:8443/jspui/handle/10603/454832 (last visited Nov 1, 2023).

[32] Right to privacy and Data Protection Era (no date) Legal Service India - Law, Lawyers and Legal Resources. Available at: https://www.legalserviceindia.com/legal/article-10664-right-to-privacy-and-data-protection-era.html

 [ISSN 2581-5369]

rights is paramount, respecting individuals' privacy rights in data handling. The principle of purpose limitation underscores that data should only be collected for specific, well-defined purposes.

Moreover, effective privacy and data protection in the digital era rely on a combination of transparency, security, education, and adherence to legal and ethical standards.[33] Organizations must continually assess and adapt their practices to address evolving privacy concerns and regulatory changes in an increasingly digital world.

VIII. ENHANCEMENT OF DATA PROTECTION LEGISLATIONS IN INDIA

The Information Technology Rules, 2011 (IT Rules, 2011) provide an overview of the current privacy legislative framework that regulates the "collecting, receiving, possessing, storing, dealing, handling, retaining, using, transferring, disclosing sensitive personal data or information, security practices and procedures for handling personal information." The right to privacy and data protection was established as a fundamental right by the Supreme Court of India in the case of *Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)*[34], and in the current legislative framework of privacy outlined in the [35]which regulates the "collecting, receiving, possessing, storing, dealing, handling, retaining, using, transferring, disclosing sensitive personal data or information, security practices and procedures for handling personal information". Its failure to address a number of important issues makes the provision in question widely viewed as insufficient. It does not cover how the state handles personal data because, first of all, it presumes that privacy is a legal right, leaving potential gaps in data protection. Furthermore, it only recognizes a limited set of data types that require safeguarding, potentially leaving many other sensitive data categories unprotected. In addition, it places minimal responsibilities on data controllers, and these responsibilities can even be waived through contractual agreements, which could compromise the privacy of individuals. Lastly, the provision lacks stringent punitive measures for those who breach data protection regulations, raising concerns about the effectiveness of enforcing data privacy laws. In summary, the provision's insufficiency is apparent on four levels, encompassing its conceptualization of privacy, data coverage, responsibilities, and penalties for offenders.

[33] Ibid.

[34] Justice K.S.Puttaswamy(Retd) vs Union of India on 26 September, 2018, https://indiankanoon.org/doc/127517806/

[35]Notification New Delhi, the 11th April, 2011 - Ministry of Electronics ..., https://www.meity.gov.in/writereaddata/files/GSR314E_10511%281%29_0.pdf .

- **Personal Data Protection Bill, 2018**

In 2018, the Justice Srikrishna Committee of the Ministry of Electronics and Information Technology (MeitY) drafted the initial draft of the Personal Data Protection Bill. Due to a number of important issues, additional revisions were required in India. The requirement pertaining to data localization was one of the main points of contention. Within an Indian server or data centre, data fiduciaries are required to hold at least one duplicate copy of customer data. The main goal of this requirement was to expedite the access of law enforcement to this kind of information.

The bill's provision for the management of personal data under legal protocols in the context of state security raised another important concern. The handling of individual information for purposes connected with the location, examination, and indictment of crime or other lawful infractions was likewise allowed. Given the shortcomings of India's current legislation pertaining to governmental monitoring, these provisions have sparked worries about the possible effects on the right to privacy. Moreover, criticisms were levelled at the regulatory framework of the draft legislation, mainly due to its apparent lack of autonomy. It seemed to be greatly impacted by the federal government and vulnerable to being swayed by commercial interests. Notably, the act gave. the authority to select the members of the Data Protection Authority, with appointments being limited to a five-year term, granted by the central government. This constrained timeline prompted questions about the authority's capacity to establish the requisite independence for effective regulatory functioning within these constraints.[36]

- **Personal Data Protection Bill,2019**

This was followed by the Personal Data Protection Bill, 2019[37], A proposed law by the Indian Parliament, known as the Personal Data Protection Bill (PDP Bill 2019), was later retracted. In addition to discussing methods for safeguarding personal information, the bill suggests creating an Indian Data Protection Authority. Key provisions that were absent from the 2018 draft bill have been included in the 2019 bill, including the ability to ask for the erasure of personal data and the government of India’s power to exclude any government agency from the Bill.

[36]Personal Data Protection bill, https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill ,2018.pdf .

[37]Times Of India, Centre withdraws personal data protection bill, 2019: Will present new legislation, says it minister: India News - Times of India The Times of India (2022), https://m.timesofindia.com/india/centre-withdraws-personal-data-protection-bill/amp_articleshow/93323625.cms .

 [ISSN 2581-5369]

- **Actions Taken in favour of Data Protection in 2020**

  a. Chinese App Ban: In 2020, the Indian government enforced a prohibition on numerous mobile applications of Chinese origin, citing apprehensions regarding national security and the protection of data. Popular platforms such as TikTok, WeChat, and UC Browser were among the apps that faced this ban. This action emphasized the immediate requirement for enhanced data protection laws in India and emphasized the value of secure management and storage of personal data.[38]

  b. Establishment of the National Cyber Security Coordinator[39]: In the year 2020, Indian government set up the National Cyber Security Coordinator (NCSC) to supervise the country's cybersecurity strategy. and facilitate cooperation among various government agencies. The NCSC is tasked with formulating cybersecurity policies and guidelines, as well as responding to cyber threats and incidents.

  c. The COVID-19 pandemic has underscored the importance of privacy and data protection. Governments worldwide have introduced contact tracing and surveillance measures to track the virus's transmission. In India, the government introduced various digital initiatives to monitor COVID-19 cases and vaccine distribution, prompting worries regarding data privacy and security. This crisis has emphasized the necessity for stronger legal structures to protect personal data and guarantee its safe handling and storage.

- **Data Protection Bill, 2021**

In 2021, the Data Protection Bill, was introduced by committee. This bill was designed to cover both personal as well as non-personal data. The committee's suggestion to require all data to be stored locally was met with some uncertainty. Additionally, the bill proposed the creation of a data protection authority, though it was later withdrawn. The bill also aimed to establish rules for the international transfer of data, hold data processors accountable, and provide remedies for unauthorized or harmful data use.[40] It also suggested protecting the rights of those whose

[38]Business news, chinese apps ban: Centre issues order to ban 54 Chinese apps - The Economic Times, https://m.economictimes.com/tech/technology/union-government-issues-fresh-orders-to-ban-over-54-chinese-apps/amp_articleshow/89551062.cms

[39] Right to privacy and Data Protection Era, Legal Service India - Law, Lawyers and Legal Resources, https://www.legalserviceindia.com/legal/article-10664-right-to-privacy-and-data-protection-era.html

[40] Government withdraws data protection bill, 2021, The Economic Times, https://economictimes.indiatimes.com/tech/technology/government-to-withdraw-data-protection-bill-2021/articleshow/93326169.cms

 [ISSN 2581-5369]

data is being handled and providing definite rules regarding the use of personal information.

- **Digital Personal Data Protection Bill, 2022**

The Digital Personal Data Protection Bill (DPDP Bill, 2022) brought about a paradigm shift in the handling of private data that has been converted into digital form, both online and offline. This comprehensive legislation now places stringent regulations on any digital processing of personal information, impacting various facets of data protection and privacy.[41]

Firstly, it's vital to understand that the DPDP Bill, 2022 extends its purview to encompass personally identifiable information, which may have been collected through online or offline means and subsequently digitized for processing. This implies that regardless of how or where personal data was originally gathered, if it's in digital form, it falls under the ambit of this bill.

Notably, this legislation holds far-reaching consequences, particularly for Indian start-ups venturing into global markets. By implementing this bill, India is enhancing legal protections for its citizens' personal data when processed abroad. This, in turn, can impact the competitiveness of Indian start-ups, as they must adhere to more stringent data protection standards when dealing with international customers and their data.

However, it's interesting to note that while the DPDP Bill, 2022 appears to bolster the privacy rights of Indian citizens globally, it paradoxically provides exemptions for Exemption for information guardians in India who process individual information of Indians. might be seen as a regulatory strategy to ensure that businesses within India are not overly burdened with compliance requirements, while still securing the data of Indian citizens abroad.

Lastly, The DPDP Bill was in its preliminary draft phase and is expected to be submitted for approval to the Indian parliament in the forthcoming 2023 parliamentary session. This legislative procedure demonstrates the government's dedication to confronting the changing complexities of the digital era regarding data protection and privacy, impacting both the domestic and international arenas.

- **Digital Personal Data Protection Act,2023**

The Digital Personal Data Protection Act,2023, which became operative on August 11, 2023, is an extensive legislative framework in India designed to protect people's rights to privacy and data in the digital age. This law has a broad scope, encompassing digital personal data processing both within and outside of India if it pertains to providing goods or services within

[41]The Digital Personal Data Protection bill, 2022 Chapter 1: Preliminary ..., https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Protection%20Bill%2C%202022.pdf

 [ISSN 2581-5369]

the country. It places a strong emphasis on obtaining lawful consent before processing personal data, with exceptions made for legitimate purposes like voluntary data sharing and government-related functions. The Act mandates data fiduciaries to uphold data accuracy, maintain security, and delete data when its purpose is fulfilled. Individuals are granted several rights, including access to their data, correction of inaccuracies, data erasure, and mechanisms for addressing data-related grievances. To balance privacy with national interests, government agencies may be exempted from specific provisions under certain circumstances, such as national security and crime prevention. This legal framework represents a substantial stride in India's endeavours to safeguard the digital personal data of individuals and bolster data security and privacy. The Indian government established the Data Protection Board, will handle non-compliance issues with the Bill.[42]

The Digital Personal Data Protection Act,2023 described in statement, appears to introduce a new era of data privacy legislation in India. This law establishes the expectations for compliance by data fiduciaries, those responsible for collecting and processing digital data, in their dealings with data principals, the individuals to whom the data pertains. While the enactment of such a law may bring relief, particularly in a time when AI-driven applications reliant on vast amounts of personal data are on the rise, it also raises several concerns and leaves important questions unanswered. Notably, the law appears to lack provisions that regulate the purposes Regarding the data that can be gathered and the permissible manner of its utilization, as long as the objective is legal. The absence of such restrictions may be a matter of concern, as striking a balance between data privacy and enabling legitimate data uses is a challenge in data protection legislation. The law permits information trustees to gather information for any legitimate explanation as long as it follows all pertinent lawful prerequisites. This Implies that practices involving algorithms that display ads and monitor individual preferences based on personal data and online behaviour (often referred to as dark patterns) can operate without significant constraints, except when it comes to children. Due to the absence of India's Digital Markets Act and the lack of regulations governing AI-based applications, the utilization of data for purposes that are legal but ethically questionable can continue to expand in India. It is legally required for parents or guardians to give their consent when their children are involved, but it is unclear how this consent can be consistently obtained. The efficacy of this legislation is contingent upon Indian nationals being cognizant of their entitlements and employing the complaint redressal system instituted under the Act. Interestingly, this act does not require the Data Protection Board

[42] Digital Personal data protection law , Request rejected, https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023,pdf

 [ISSN 2581-5369]

or other authorities to perform compliance audits of data fiduciaries or processors or to inform the public about their rights under the DPDP Act. Additionally, there is no requirement for proactive measures to mitigate potential harm. Consequently, despite its good intentions, the DPDP Act lacks the essential mechanisms for enforceability.

The DPDP Act's Section 8(5) requires data fiduciaries to implement reasonable security measures to prevent breaches of personal data within their purview. However, the legislation does not provide a clear definition of what constitutes "reasonable security measures." The question of whether these security measures should be proportionate to the associated risks remains unresolved. It is anticipated that the regulations accompanying the DPDP Act will address these concerns.

Nevertheless, until this clarification occurs, there is a valid concern that the term "reasonable" may potentially weaken the requirement for safeguarding vigorous information security rehearses as presented by the DPDP Act is essential. Additionally, When comparing the DPDP Act to the Right to Persons with Disabilities Act, 2016, there are some differences. The DPDP Act stipulates in Section 9(1) that data fiduciaries must obtain authenticated consent from the legal guardian before handling the personal information of people with disabilities.

This may seem to contradict the recognition of legal capacity for people with disabilities, as outlined in Section 13 of the RPWD Act. The perplexity deepens when we examine Section 38, which seems to present conflicting provisions. While Section 38(1) indicates that the DPDP Act should complement rather than override other existing laws, Section 38(2) suggests that in case of a conflict, The DPDP Act will prevail in cases of conflict.

Concerning individuals with disabilities, Uncertainty surrounds the necessity of guardian consent in all cases and the circumstances under which an individual's legal capacity will be accepted. This raises questions about how to interpret the DPDP Act alongside the RPWD Act in a harmonious manner.

As the judicial system tests and deliberates over the provisions of the DPDP Act, it is expected that a large number of these uncertainties will be cleared up. In the meantime, there is hope that the Ministry of Electronics and Information Technology (MEITY) will proactively amend the law or issue rules to provide much-needed clarity.[43]

[43]The Digital Personal Data Protection Act, 2023: Some relief but many questions, Times of India Blog (2023), https://timesofindia.indiatimes.com/blogs/niveditas-musings-on-tech-policy/the-digital-personal-data-protection-act-2023-some-relief-but-many-questions/

 [ISSN 2581-5369]

IX. Recommendations/Suggestion

Every day, millions of people in India use various apps, and in doing so, they leave behind digital traces that can be potentially misused for things like creating user profiles, targeting advertisements, and making predictions about their behaviour. In India, the legal framework for handling this data is complex, with different laws governing different aspects of it. This complexity contributes to uncertainty and is a significant factor in data breaches. The population of over 1.3 billion people faces the risks of cybercrime, emphasizing the critical need for privacy and data protection.

There's a clear need to update and assess the many missing or dysfunctional complaint resolution mechanisms. Bringing individuals or organizations responsible for data breaches and cybersecurity violations to justice in India is often hindered by various challenges in implementation. As a nation, India sees its citizens' data as a valuable resource, and depending on national security and geopolitical goals, there may be a requirement to keep this data within the country's borders. This applies not only just to businesses but also to NGOs and government entities. Online transactions require special attention and should not rely solely on the guidelines provided by the Reserve Bank of India (RBI).

Technology becomes outdated even before it's introduced, and India urgently needs comprehensive laws to address a wide range of concerns, including online banking, rules for publishing content, Online slander, digital terrorism, digital currency, and non-fungible tokens (NFTs). These concerns are also crucial for businesses that want to safeguard customer information in an increasingly digital age in order to keep customers' trust and their market share. The government must collect and use data to provide essential services like healthcare, education, and public services. However, at the same time, it must make sure that the integrity of the data is maintained and that no unauthorized access or misuse occurs to this information. Considering all these factors, privacy is a fundamental right that needs to be preserved and protected. Protecting privacy is a significant effort because it represents one of our most basic rights.

X. Conclusion

Sharing personal information for security is essential in today's world, but in India, there's a pressing need for more robust laws to safeguard our data effectively. While some amendments have been made to the IT Act, it's crucial to balance defending the public interest with thwarting the growing tide of cybercrimes. It is now acknowledged that privacy is a fundamental right., but rapid technological advancements have raised questions about the extent of our privacy.

 [ISSN 2581-5369]

Technology has brought both benefits and threats. Cybercrimes, data theft, and misuse have become prevalent, directly impacting our privacy. India currently lacks sufficient Data Protection Laws, even though there are related legislations such as the IT Act, Criminal Law, and Intellectual Property Law. These laws have gaps, and stringent Data Protection Laws are necessary to ensure data privacy.

Although the Supreme Court has acknowledged in accordance with Article 21 of the Constitution, privacy is a fundamental right., raising awareness of this right and establishing effective avenues for redressal is crucial. Data privacy should also be considered alongside personal privacy. The government needs to set up mechanisms for swift action and enact laws that secure the handling of collected data, imposing significant penalties for unauthorized access or misuse

As an alternative to collecting biometric information, some experts propose smart cards as a secure option. Smart cards require a PIN, ensuring active citizen participation in the identification process, and reducing the risk of unauthorized access to biometric databases.

Ensuring In the digital age, protecting privacy and data is complicated. Fairness and transparency in the gathering and use of data are essential, and people should be aware of the purposes for which their data is being gathered. Data must be kept confidential and used only for its intended purpose, and Everybody should be able to view and edit their data.

Hence, it is crucial to safeguard personal information effectively, promote a secure environment for citizens, and encourage foreign investment without concerns about data vulnerability.

*****

 [ISSN 2581-5369]

XI. REFERENCES

- Jayanta Boruah & Bandita Das, Right to privacy and data protection under Indian legal regime SSRN (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3827766.
- Sumedha Ganjoo, Right to privacy and data protection laws in India balancing rights and managing conflicts Shodhganga@INFLIBNET: Right to Privacy and Data Protection Laws in India Balancing Rights and Managing Conflicts (1970), https://shodhganga.inflibnet.ac.in:8443/jspui/handle/10603/440613?mode=full
- Vijay Pal Dalmia, Data Protection Laws in India - everything you must know - data protection - india Data Protection Laws In India - Everything You Must Know - Data Protection - India (2017), https://www.mondaq.com/india/data-protection/655034/data-protection-laws-in-india---everything-you-must-know
- M. P. Sharma and others vs Satish Chandra, district on 15 March, 1954, https://indiankanoon.org/doc/1306519/
- Kharak Singh vs the state of U. P. & others on 18 December, 1962, https://indiankanoon.org/doc/619152/
- Govind vs state of Madhya Pradesh & ANR on 18 March, 1975 https://indiankanoon.org/doc/436241/
- Malak Singh Etc v. State of Punjab & Haryana &others on 5 December 1980 https://indiankanoon.org/doc/971635/
- R. Rajagopal vs state of T.N on 7 October, 1994 https://indiankanoon.org/doc/501107/
- People’s Union of Civil Liberties ... vs Union of India (UOI) and ANR ..., https://indiankanoon.org/doc/31276692/
- Justice K.S.Puttaswamy(Retd) vs Union of India on 26 September, 2018, https://indiankanoon.org/doc/127517806/
- Right to privacy and Data Protection Era, Legal Service India - Law, Lawyers and Legal Resources, https://www.legalserviceindia.com/legal/article-10664-right-to-privacy-and-data-protection-era.html
- Data Protection Laws in India, Data Protection in India- India Law Offices, https://www.indialawoffices.com/legal-articles/data-protection-laws-in-india

 [ISSN 2581-5369]

- Sneha Mahawar, Data Protection Laws in India iPleaders (2023), https://blog.ipleaders.in/data-protection-laws-in-india-2/
- Eprocure.gov.in, https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMTk4NzY=
- Akshhatha Adarssh, A comparative study of right to privacy as a human right with special reference to India United Kingdom and USA Shodhganga@INFLIBNET: A Comparative Study Of Right To Privacy As A Human Right With Special Reference To India United Kingdom And USA (1970), https://shodhganga.inflibnet.ac.in:8443/jspui/handle/10603/454832
- Griswold v. Connecticut, 381 U.S. 479 (1965) (no date) Justia Law. Available at: https://supreme.justia.com/cases/federal/us/381/479/
- Sanctity of personal data: A Comparative Study of data privacy laws in ..., https://thelawbrigade.com/wp-content/uploads/2020/05/Anisha-IJLDAI.pdf
- The aadhaar (targeted delivery of financial and other subsidies ..., https://uidai.gov.in/images/Aadhaar_Act_2016_as_amended.pdf .
- Notification New Delhi, the 11th April, 2011 - Ministry of Electronics ..., https://www.meity.gov.in/writereaddata/files/GSR314E_10511%281%29_0.pdf
- Personal Data Protection bill, https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf
- Times Of India, Centre withdraws personal data protection bill, 2019: Will present new legislation, says it minister: India News - Times of India The Times of India (2022), https://m.timesofindia.com/india/centre-withdraws-personal-data-protection-bill/amp_articleshow/93323625.cms .
- Business news, chinese apps ban: Centre issues order to ban 54 Chinese apps - The Economic Times, https://m.economictimes.com/tech/technology/union-government-issues-fresh-orders-to-ban-over-54-chinese-apps/amp_articleshow/89551062.cms
- Government withdraws data protection bill, 2021, The Economic Times, https://economictimes.indiatimes.com/tech/technology/government-to-withdraw-data-protection-bill-2021/articleshow/93326169.cms
- The Digital Personal Data Protection bill, 2022 Chapter 1: Preliminary ...,

 [ISSN 2581-5369]

https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Protection%20Bill%2C%202022.pdf

- Digital Personal data protection law, Request rejected, https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023,pdf
- The Digital Personal Data Protection Act, 2023: Some relief but many questions, Times of India Blog (2023), https://timesofindia.indiatimes.com/blogs/niveditas-musings-on-tech-policy/the-digital-personal-data-protection-act-2023-some-relief-but-many-questions/

*****

 [ISSN 2581-5369]