International Journal of Law in Changing World

Volume 3 Issue 2 (2024) ISSN 2764-6068

Research article
JNL: https://ijlcw.emnuvens.com.br/revista
DOI: https://doi.org/10.54934/ijlcw.v3i2.84

THE DIGITAL PERSONAL DATA PROTECTION ACT OF 2023: STRENGTHENING PRIVACY IN THE DIGITAL AGE

Shubham Saurabh
Gujarat National Law University, Gandhinagar, Gujarat

Article Information:

Received
January 30, 2024
Reviewed & Revised
May 21, 2024
Accepted
December 5, 2024
Published
December 29, 2024

Keywords:

digital personal data,
data security,
data fiduciary,
right to be forgotten,
data consumption

ABSTRACT | 摘要 | RESUMEN

The Digital Personal Data Protection Act of 2023 is a landmark piece of legislation that safeguards individual privacy rights and strengthens data security. It emphasizes the power of individuals over their personal data by introducing the concepts of consent, data minimization, and the right to be forgotten. The Act also impacts businesses by imposing obligations on data controllers and processors, requiring them to implement effective data protection frameworks and procedures. The Establishment of the Data Protection Board of India as the Central Watchdog will be crucial in enforcing the Act. This research paper examines the power given to people over their personal data and its impact on business compliance and operational changes on data controllers, given the penalties for non-compliance. The analysis concludes that the Digital Personal Data Protection Act of 2023 serves as a beacon for privacy rights and data protection in the digital world.

FOR CITATION:

Saurabh, S. (2024). The Digital Personal Data Protection Act of 2023: Strengthening Privacy in the Digital Age. International Journal of Law in Changing World, 3 (2), 77-94. DOI: https://doi.org/10.54934/ijlcw.v3i2.84

1. INTRODUCTION

Personal Data, is an inherent and inalienable characteristic of human being. It speaks about that individual, how he/she will be recognized in a society [8]. This can be anything which links to that person or individual that helps in identifying that person is his personal data. This can be name, surname, e-mail address, phone number, or even your choices regarding any book, food, political ideologies etc. This makes the personal data, the most vulnerable thing in this digital era. Companies as well as that process these personal data usually provide their services free of cost [9]. This processing of personal data helps in understanding human behaviour, tastes patterns about that particular individual, which helps them to create targeted ads that they can sell and generate revenue. The unchecked or unregulated processing of these personal data may have a dire or unpredicted results which not only violate the basic fundamental "right to privacy"[1] of that individual guaranteed under "Article 21 of the Constitution of India"[2], but also shows the inability, incompetency or lack of government will to protect the fundamental rights of their citizen.[3] The idea of data protection has roots in several different nations. The European Union law i.e General Data Protection Regulation is one such law which can be the champion in data protection all around the world.

The enactment of law for regulating this personal data protection is a complex exercise which requires a careful approach to balance the privacy concern at one hand and legitimate State interest at the other hand.[4] In order to make the reality of landmark judgment of the Supreme Court of India in "Justice K.S. Puttaswamy (Retd) v. Union of India"[5], "the Digital Personal Data Protection Act, 2023" was enacted by the government on 11th August, 2023. The fundamental idea behind this was to recognise both the "right of individual to protect their personal data" and "the need to process such personal data for lawful and legitimate purposes."[6]

[1] *Justice K.S Puttaswamy (Retd) v. Union of India*, (2017) 1 SCC 10

[2] *Constitution of India (1950)*, art 21

[3] *Supra* note 2 at 56

[4] *Supra* note 2 at 58

[5] *Supra* note 2 at 127

[6] *The Digital Personal Data Protection Act, 2023*, (Act 22 of 2023).

https://doi.org/10.54934/ijlcw.v3i2.84

The Act applicable to the administration of digital personal data across India, whether obtained via the Internet or otherwise. There are some exemptions given in the Act as well like data processing by the instrumentalities of the State such as national security. The Act does not even recognize the consequences or harms arising from processing of personally identifiable information. Right to be removed (forgotten), principle of consent, Data Protection Board of India are some of the key component or highlights where it is helpful in understanding the function measures taken by the government to control the illicit use of personal data by data fiduciaries.

One another key component that makes this Act a major boost for strengthening the right to privacy is the amount of penalty that may be imposed on data fiduciaries if they are found guilty of violating the provisions of this Act.

Before this Act, India does not have any stand-alone legislation that talks about the data protection. The recognition of personal data as a "right to privacy" necessitates the urgency for having a separate law for regulating the processing of personal data especially in digital platform. The work on this Act began nearly a years after the Puttaswamy, when the union government established an expert committee on Data Protection, chaired by Justice B.N Srikrishna, to review and explore data protection problems and difficulties in our nation-state. In July 2018, the committee present its report. The Personal Data Protection Bill, 2019 was introduced in Lok Sabha in December 2019 at the Committee's proposal,[7] the bill was later withdrawn from Parliament due to report submitted by Joint Parliamentary Committee. Then bill was released for public opinion in November 2023.[8] The Digital Personal Data Protection Bill, 2023 was reintroduced into Parliament in August 2023 and got its assent by the President on 11th August 2023.[9]

Data Processing of personal data in digital realm will only be done through the letters of this Act and obviously for lawful and legit purpose. This research paper will try to examine the power given to people over their personal data, process of consent, right to be forgotten, and its impact on business and organisation in terms of compliance and operational changes, obligation on data controllers, "data

[7] Pre-Legislative Research, https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023 (Last visited Oct 5, 2024)

[8] *id*

[9] *See Supra note 8*

https://doi.org/10.54934/ijlcw.v3i2.84

protection board of India," penalties for non-compliance. The data protection is the authority for the "right to privacy" [2].

2. THEORETICAL BACKGROUND

2.1. Right to Privacy and Data Protection

When the United States East Coast had seen unusually intensive urbanization, Warren and Brandeis formulated the concept of the right to privacy. The period between 1790 and 1890 witnessed a rise of the US population from 4 million to 63 million. More than 8 million people had immigrated to the US by 1890. Rapid technological advancement and innovation have put pressure on the private sphere and being under stress [3, 4]. "The right to privacy" is a part of human dignity and guarantees that a person can live with dignity by protecting the private information of their personality from unauthorized access. Individual autonomy and freedom to make crucial decisions that have an impact on one's life are both recognized by privacy. This postulates the reservation of a private space for the individual, described as the right to be let alone. Every person is born with the inherent right to privacy, which is essentially a natural right. Such a right belongs to every human being till the last breath is taken. It does go hand in hand with human beings and is unalienable from them. It emerges from the human body and dies with the human body.[10]

The "right to privacy" in the digital sphere can be preserved by the way of data protection. The concepts of privacy and data protection are intertwined historically. At the most fundamental level, data protection is largely predicated on how Article 8 of the European Convention on Human Rights is interpreted, but in practice, these two rights are still muddled. Moving from what sets the right to data protection apart from the right to privacy seems like a good place to start when trying to define the essence and justification of the right to data protection [4, 5].

Between data protection and the right to privacy, there is one key distinction. By referencing their role within the constitutional state, this distinction is made on teleological grounds. The right to privacy is a "tool of opacity" that shields people from government and private actors' intrusion by forcing them to

[10] *See supra* note 2 at 134.

https://doi.org/10.54934/ijlcw.v3i2.84

refrain from unwanted action. By establishing normative boundaries for it, privacy restricts authority. On the other hand, data protection primarily serves as a "tool of transparency," regulating and channelling the exercise of power rather than putting a stop to it [10].

2.2. Concept of Personal Data

"Personal Data"[11] is any piece of information that is connected to an "identified or identifiable living individual."[12] This can be scattered pieces of data that may be joined together and then result in the determination of a specific person and the creation of private information. Personal data that is completely anonymous in a way that is no longer useful to identify a person is not personal data. The definition given under the Act is very precise in determining any data as personal data. Designation, surname, place of residence, e-mail, identification card number (AADHAR NUMBER), mobile number, Internet Protocol address (IP), and so on are some basic illustrations of "Personal data." The prime motive of this Act is to safeguard these data from being misused by any data processing entity. However, the law is helpless in a case when your personal data is publicly available and with your consent. Let's take a hypothetical situation: Mr. A is an individual who makes video content for any digital platform, say for example X. In doing so, Mr. A negligently or carelessly disclosed his personal details, such as his home address or e-mail address. Then, in this situation, Mr A can't claim or seek the protection of this law for being spammed by any particular company over his e-mail address.[13] The general notion among citizens is that once the law is passed, no one can use their personal data. Still, the thing is their data is being used and processed by data processing companies because their personal data are publicly available to those companies. They don't need your consent in this situation to process data for their benefit. To avoid this kind of situation one always needs to be careful and vigilant in digital space about whatever they are posting and how it is related to their personal data.

2.3. Components of Consent

Consent is the basic aspect of human interaction. It gives autonomy to an individual over his rights that can be exercised by them like natural rights, fundamental rights, statutory rights, customary rights etc

[11] "*The Digital Personal Data Protection Act, 2023*, § 2(t), No. 22, Acts of Parliament, (India)"

[12] *id*

[13] "*The Digital Personal Data Protection Act, 2023*, § 3(c), No. 22, Acts of Parliament, (India)"

https://doi.org/10.54934/ijlcw.v3i2.84

[6, 7]. This protects the individuality of a person that makes them different from others [5]. Consent helps to recognise the will that a person exercises from their own, and this needs to be protected. Rather, it is the responsibility of the State to safeguard the consent of its citizen. In that light various components of consent have been integrated into the Act. Some of the major elements of Consent are:

1. Consent must be without duress, exact, informed, without conditions and incontestable and limited to such purpose only for which consent was given.[14]

2. Consent infringing the letters of any law shall not be consent at all.[15]

3. Every consent form presented to an individual (Data Principal)[16] must be in clear, plain and in a language understandable by the individual, together with the particulars of the "Data Protection Officer."[17]

4. Withdrawal of consent shall be as easy as when the consent was given. (Right to withdrawal of consent).[18]

5. Consequence of withdrawal shall lie upon the individual itself.[19]

6. The burden of proving that consent was given to process personal data shall lie upon the Data Fiduciary.[20]

[14] "*The Digital Personal Data Protection Act, 2023*, § 6(1), No. 22, Acts of Parliament, (India)"

[15] *Id.* § 6(2) *note 21*

[16] Id § 6(3) note 21; *See also*, Data Principal means the individual to whom the personal data relates.

[17]*id*, § 6(3) note 21; "Data Protection Officer means an individual appointed by the Significant Data Fiduciary" § 2(i); "Significant Data Fiduciary means any Data Fiduciary as may be notified by the Central government" § 2(z)

[18] *id* § 6(4) note 21.

[19] *Id* § 6(5) note 21

[20] *Id* § 6(10) note 21; *See also "*Data Fiduciary means any person alone or in conjunction with other person determine the purpose and means of processing of personal data."

https://doi.org/10.54934/ijlcw.v3i2.84

The above components of the consent clearly empower the data principal over their personal data. It gives immense authority ranging from the manner to get consent to transferring the burden to prove that consent was given to data fiduciaries as per the provisions of the law. These components strengthen an individual's overall privacy control over their personal data in the digital space. These components also put extra burden on data fiduciaries to make themselves aware of their compliance with this law or face severe consequences.

2.4. Rights and Duties of Data Principal

"Data Principal" is the person whose personal data is being collected, stored, and processed by the Data Fiduciary to offer their services. The components of consent clearly show the value of personal data and the autonomy given to data principal concerning their personal data. It is as if "my data, my will" and this also helps strengthen the overall pillars of the right to privacy. However, apart from all these, there are certain sets of rights and duties that the data principal must know before granting their consent to process personal data. First, let us understand the rights that are available to data principal.

2.4.1 Right to inspect private information.

Data principals are given the right to inspect their private information, for which they have originally given consent for processing. Data principals can get a summary of private information, details of all other "data fiduciaries" and "data processors" with whom the private information was shared, and any other information that may be directly or indirectly related to that personal data.[21]

2.4.2 Right to rectify and deletion of "personal data"

The individual or Data Principal being the sole owner of their personal data gives them the undisputed authority to check whether the shared data received by the data processor is correct or not. In case the information is not correct or does not give a complete idea about the individual, the data principal shall have the right to rectify the collected data. The data processor shall, on the demand of the individual, either edit the wrong or misleading data and correct the incorrect data or update the private data.[22]

[21] DPDP Act 2023, § 11

[22] DPDP Act 2023, § 12

https://doi.org/10.54934/ijlcw.v3i2.84

Every individual shall have the power to get their personal data deleted from the database of the data processor, and the company or organisation shall delete that information within a reasonable amount of time. This right strengthens individual control over their personal information, ensuring that it is not only accurate but also kept in line with their current preferences and consent. Organizations handling personal data are statutorily bound to respect and facilitate these rights, enhancing individuals' privacy and data protection in an increasingly digital world.

2.4.3 Right of Grievance Redressal.

This right enhances the mechanism adopted in the Act by putting an extra obligation on the data fiduciary to be available to register any grievance by the data principal. The company or organisation, through its appointed official, must respond to any of the issues in a time-bound manner that may be prescribed with time. It is the duty of the Data Principal to exhaust all the rights of the grievance redressal mechanism offered by the data fiduciary before approaching the Data Protection Board of India.[23]

This may increase the time to get things done for the aggrieved data principal, but this also has an advantage as it helps to solve the issues at the preliminary level. It is a two-way sword for both the individual and the data processor.

2.4.4 Right to nominate

This right helps the individual secure their data in case they cannot make the decision themselves because of an unforeseen event. The data principal can nominate any other individual who will be solely responsible for deciding on that person's data.[24]

This right ensures that an individual can specify a trusted person or entity who will have the power to make decisions or receive the perks on their behalf if they are unable to do so by themselves. This is as if the power of attorney given in case of sale of immovable property where the owner appoint any person as power of attorney who shall exercise all the duties on behalf of the owner. Still, there is a slight difference in both concepts as in power of attorney the owner can do all those things that the person appointed will

[23] DPDP Act 2023, § 13

[24] DPDP Act 2023, § 14

https://doi.org/10.54934/ijlcw.v3i2.84

do. Still, in case of nomination, the data principal must be in a situation where they are not able to exercise their mind over personal data.

All these above points ensure the rights of the data principal over their personal data. Now, let us examine some of the general duties that they must be vigilant about while exercising the protection of the law. The duties enshrined under the Act are:

- Be within the boundary of law while exercising the right over personal data as no one is above the law.[25]
- Not to impersonate any other person over digital space because impersonation is a criminal offence under the country's penal laws.[26]
- Not to conceal significant information while providing personal information like duplicating the identity proof of address issued by an appropriate authority.[27]
- Avoid filing unnecessary complaints with "Data fiduciary" or "Board".[28]
- To show or produce only true and authentic data while exercising the right to rectification or deletion under the law.[29]

2.5. Obligations of Data Fiduciary

Data fiduciaries are those entities primarily responsible for collecting, storing, and processing data. The Act puts some obligations that these entities must follow to avoid any penalties from the Data Protection Board of India. These obligations are somewhat duties that they must abide by. The nature of this obligation is such that even if there is no agreement between Data Principal and Data Fiduciary, the Data fiduciary is responsible for following the letters of this law or any regulation made or prescribed

[25] DPDP Act 2023, § 15(a)

[26] *Id* § 15(b) note 32

[27] *Id* § 15 (c) note 32

[28] *Id* § 15(d) note 32

[29] *Id* § 15(e) note 32.

https://doi.org/10.54934/ijlcw.v3i2.84

whenever they are processing the individual's personal data. Some of the key obligations of these entities are listed below:

- Any Data Fiduciary engaged or involved in Data processing of personal data to offer any goods or services to that person shall do so only under a valid contract.[30]

This means there must be a valid contract between individuals and data processors for the processing of personal data. Let's assume an insurance company X offers services of life insurance to their clients. Then, that company must have personal data of many of its clients. In order to process those data, a valid contract must be established between insurance company X and its clients. The contract must clearly mention in the terms the motive for which personal details are getting ground by the company.

- If a company or organisation is taking any decision that will ultimately affect the data principal or disclose their personal data to another data fiduciary, then the data processer must ensure its authenticity, precision and persistency of the private details.[31]

Let me put this in another way: imagine a person named Ram who applies for a loan on an online lending platform. The platform, acting as a Data fiduciary, collects and processes Ram's personal data, including his financial history, employment details and credit score. The online lending platform uses Ram's personal data to assess his creditworthiness and decide whether to approve the loan application. This decision significantly affects Ram as it will help him get a loan, which might be critical for him. In such a situation, the lending platform is duty-bound to produce the personal details in complete, exact, and consistent with Ram's.

- The organisation must protect the private details in its holding or under its authority.[32]
- An entity must implement a reasonable security measure to prevent any data breach in data in its possession.[33]

[30] DPDP Act 2023, § 8(2)

[31] *Id* § 8(3) note 37

[32] *id* § 8(5) note 37

[33] *id*

https://doi.org/10.54934/ijlcw.v3i2.84

- Even after taking all the security measures, if a data breach of personal data occurs, then it shall be the duty of the data fiduciary to inform the data principal of such breach of information. The intimation information letter must cover the breached data and how it affects the data principal.[34]

- Duty to erasure the personal data within a reasonable period of when the purpose for which the data was collected ceases to exist or when the data principal has withdrawn the previous given consent.[35]

- An individual must be appointed as the sole point of touch between the data fiduciary and the data principal.[36]

- Entities must implement an effective grievance redress mechanism for the data principal.[37]

Apart from these general obligations upon data fiduciaries, the central government can impose additional obligations on significant data fiduciaries when assessing any other relevant factors. This may include an independent data auditor who shall be responsible for performing the data auditing[38] and analysing the adherence mechanism of "Significant Data Fiduciary."

3. DATA PROTECTION BOARD OF INDIA

The Data Protection Board of India (DPBI) is a regulatory body that would be set-up at an appropriate place where the union government thinks fit. This corporate body is comprised of a chairperson and members appointed by the central government. The Board holds a significant and central role in compliance with DPDP. It can direct urgent measures in case of personal data breach, investigate the breach itself and impose appropriate fines. It can also issue suitable directions. Any appeal against the order or direction can be preferred before "Telecom Disputes Settlement and Appellate Tribunal

[34] *Id* § 8(6) note 37

[35] *Id* § 8(7) note 37

[36] *Id* § 8(8) note 37

[37] *id*

[38] DPDP Act 2023, § § (10)(2)(b)

https://doi.org/10.54934/ijlcw.v3i2.84

(TDSAT)"[39] within 60 days, and an appeal challenging the order of TDSAT lie only before Supreme Court of India.

DPBI has been given the authority to levy a huge monetary penalty of up to Rs. 250 crores. It will have to contemplate the seriousness, magnitude, timeline, repetitive nature of such breach, the kind and category of the private details in question, unlawful gain in committing such breach and so on while deciding the quantum of monetary compensation to be imposed.

Having a separate body responsible for regulating the breach of personal data gives in-depth understanding and helps in making informed decisions. An independent board can solely concentrate on this problem and try to solve the problems associated with data breaches. This also helps reduce the time for data principal to secure their personal data, and prompt action is possible. Specialized boards are often more open to innovation and new approaches in addressing issues. Their specific focus allows them to explore creative solutions and adapt to evolving technologies and trends in data protection.

4. IMPACT ON BUSINESS AND ORGANISATION IN TERMS OF COMPLIANCE AND OPERATIONAL CHANGES

The enactment of DPDP Act, 2023 will make a revolution in the future in terms of protecting personal data and upholding the right to privacy enshrined under Article 21. This Act will impact the data processor significantly in terms of its compliance and make them change their operational framework simultaneously. This operational framework will hurt their business activities, services, and other fundamental elements. Some of the major impacts are as follows:

4.1 Establishment of Data Protection Grievance Redressal Mechanism.[40]

The Data Fiduciaries have been statutorily mandated to establish a grievance redressal mechanism, which will serve the data principal in lodging their grievances in the form of complaint if they find that

[39]DPDP Act 2023 § 29(8); *See also,* "Telecom Regulatory Authority of India Act, 1997" § 14A & § 16, No. 24, Acts of Parliament, (India).

[40] *See supra* note at 30, 44

https://doi.org/10.54934/ijlcw.v3i2.84

their personal data is being misused, altered or used for any other purpose than that for which it was collected.

A "Data Protection Officer (DPO)" must be appointed by the business or organisation. The contact details of DPO will be publicly available. DPO shall be the only point of contact between the Data Principal and the Data fiduciary. DPO will respond to all the lodged complaints within a prescribed period and ensure the effective resolution of issues faced by the data principal. The basic idea or purpose for having a separate individual is to ensure accountability and transparency on the part of the data processor.

4.2 Executing Independent Data audit.

Executing independent data audits is an important process to analyse, evaluate and enhance the organisational data protection mechanism. This process helps in designing a robust system that will ensure accurate and efficient information on the data principal. The audit involves regularly examining data management process, data sharing and data usage within the data processor. The purpose is to identify lapses, vulnerabilities, improvement areas, and compliance with DPDP Act, 2023.

The audit would involve interviews with key personnel in data management, IT staff and the Data Protection Officer. This discussion may help auditors understand the real situation of organisational data handling processes regarding personal data protection practices. After the assessment, the data audit team will prepare a detailed report. The report will state the strengths and weaknesses of the organisation and recommend the area for improvement.

4.3 Keeping accurate personal data.

The legal obligation of an organisation to ensure true and accurate personal data of the data principal puts an extra burden on the data processor. This means the business or organisation must take appropriate steps to verify data, regularly update, cross verify, error correction and provide access to the data principal.

4.4 Ensure Informational Privacy.

Ensuring informational privacy in the digital age is a utopia, but trying to reduce it is not an impossible task. This safeguards individual sensitive information from unauthorized access. Achieving these requires businesses and organisations to implement stringent security measures, robust encryption

https://doi.org/10.54934/ijlcw.v3i2.84

protocols, and access controls within the data processor structure. Strict adherence to DPDP Act, 2023 requires an organisation to educate their employees and provide them with clear instructions about how the collected personal data can be used in a well-defined manner. Regular data audits, risk assessment, and prompt response to data breaches are essential to ensure an effective mechanism for informational privacy. These things will certainly affect entities in their operational cost; it will be interesting to see how they will manage their cost to keep offering free services to their customers.

4.5 Facilitate the right to access information

Facilitating the right to access information under the "Digital Personal Data Protection Act, 2023" means ensuring the individual has easy access to their personal data stored by the data processor. An individual, being the owner of their private details, has the right, under the Act, to know what information organisations have collected about them, for what purpose, how it will be used, and with whom the data fiduciary is sharing such data. To offer all these facilities, the business organisation must establish a mechanism such as online portals or dedicated customer service channels, enabling data principal to request their data. Data principals can even withdraw the consent given to store the data, and the data fiduciary has to delete all the collected data from their databases within a reasonable period of time.

4.6 Facilitate state instrumentalities in discharging public function.

It shall be the duty of Data Fiduciary to help the state agencies in discharging their public function. Central government may even ask to stop the transfer of personal data to outside India. This will surely impact the core business activity of data processor because their main function is being stopped here. Adjudicating body specially entrusted may direct these company or organisations handling personal details, to furnish them before their clients and they are duty bound to furnish all such data. They can't deny stating that this will go against their privacy policy. State agencies may ask personal data in the pursuit of preventing, identifying, probing or pursuing legal action against any violation or breach of the law. The general ground upon which the State and its agencies can process the personal data violating the fundamental right to privacy in safeguarding India's sovereignty and integrity, ensuring state security, fostering amicable relationships with foreign nations, preserving public order, and averting provocation leading to any recognizable offense, etc.

https://doi.org/10.54934/ijlcw.v3i2.84

5. CONCLUSIONS

In the multifaceted landscape of the digital world, data protection and privacy have never been more crucial than they are today, where data flows continuously, and technology manages every area of our lives. Data protection and privacy have now emerged as fundamental rights. The debate over these topics highlights the intrinsic balance between protecting individual rights and freedom and advanced technology. Modern technology may make people's lives more convenient and easier but sometimes causes severe threats to the privacy of the people when their data's being traded off. The integration has made the gathering and processing of enormous volumes of personal data of big data analytics, artificial intelligence, and the Internet. The digital era has enormous potential for innovation, economic expansion, and societal advancement. Still, it raises serious concerns about the exploitation and misuse of private data collected by the fiduciary.

Since we are in the realm of a data-driven era, we cannot take a chance to compromise with data privacy as the lives of the people are more entwined with the digital platform. That's why there is a need for a regulatory framework dealing with the right to privacy in the digital realm. The "General Data Protection Regulation (GDPR)" of Europe is a milestone development in the field of personal details and their protection. It was enacted in 2018, setting a standard for data protection laws worldwide. It establishes the legal framework ensuring accessibility, confidentiality and securing transparency, consent and user control. In addition, the GDPR strongly emphasizes individuals' rights to their personal data, requiring enterprises to be open and honest about how they use it, have an individual's explicit consent, and put strong security measures in place. The GDPR promoted a culture of accountability by giving people more control over their data and severely fining non-compliant businesses.

Despite global standards set out in the GDPR, cybersecurity threats are still developing and getting more advanced and focused. Malicious actors continually look for vulnerabilities in digital systems, endangering the privacy of millions of people through ransomware assaults and data breaches. The ethical ramifications of data consumption have also attracted attention. The ethical issues surrounding the acquisition, stockpiling, and use of personal details have taken centre stage in the privacy conversation. It is a difficult but necessary endeavour to balance innovation and ethics, data-driven insights and individual rights.

https://doi.org/10.54934/ijlcw.v3i2.84

In India, the year 2023 became the milestone for ages when the Parliament enacted the law on data protection with respect to privacy and data protection. Digital Personal Data Protection Act, 2023 is a step forward by the government of India in recognising the importance of securing personal digital data and information. It clearly states that the data collected can only be used for the purpose it was collected for. The Act established the Data Protection Board of India, which plays a significant role in compliance with individual personal data protection. The Board had immense power to take prompt action against anyone in case of privacy breach and protection and imposed penalties up to 250 Cr.

However, challenges and vulnerabilities still exist. The quick rate of technological advancement continuously examines the limits of existing laws. Finding a balance between innovation and privacy protection is still a struggle. Furthermore, the sophistication of cyber-attacks outburst rapidly, underscoring the need for continuous assessment of the implementation of data protection laws.

Education and awareness are recognized as effective measures for defending data privacy. It is crucial to educate people about their rights, the dangers and consequences of engaging in certain activities online, how to stay safe while doing so and most importantly, some basic information regarding what to do and what not to do while providing information online. Additionally, technological solutions also play a crucial role in preserving data.

Data security and privacy are essential components of a free, safe, and just digital society; they are not just trendy buzzwords. It is a journey, not a destination. That's why individuals, government agencies, businesses and technology creators must collectively work together to uphold these principles. It is essential for the moral and sustainable development of our digital society, that individuals have control over their personal information, data security, and privacy. A future where data and privacy are protected respected. And it will be made possible by ongoing education, lobbying, and responsive policy-making. It necessitates constant attention, flexibility, and contemplation towards morality. However, it is important to understand that the decisions we make today will have repercussions in the future. Thus, we can create a digital world where privacy is not only a right but an unalienable reality by developing a culture of respect for privacy, adopting creative yet moral solutions, and promoting education and awareness.

https://doi.org/10.54934/ijlcw.v3i2.84

REFERENCES

[1] Brandeis, S. D. (1890). The Right to Privacy. *Harvard Law Review*, 193.

[2] Bygrave, L. A. (2010). Privacy and Data Protection in an International Perspective. *Stockholm Insititute for Schandinavian Law*, 165-200.

[3] Carpenter B., O. E. (2014). Harm, Responsibility, Age and Consent. *New Criminal Law Review: An International and Interdisciplinary Journal*, 23-54.

[4] Jayanta Ghosh, Uday Shankar (2016) PRIVACY AND DATA PROTECTION LAWS IN INDIA: A RIGHT-BASED ANALYSIS, Bharati Law Review, Oct – Dec, 54.

[5] Fabbrini, F. (2014). *Fundamental Rights in Europe: Challenges and Transformations in Comparative Perspecitve.* Oxford University Press.

[6] M M S Karki (2005) Personal Data Privacy & Intellectual Property," Journal ofIntellectual Property Rights, Vol 10. 59-63.

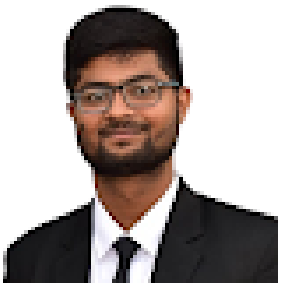
[7] P.H., S. (1994). Rethinking Informed Consent. *The Yale Law Journal*, 899-915.

[8] Shah, P. (1997). International Human Rights: A perspective from India. *Fordham International Law Journal*, 24-28.

[9] Shutova, A. (2022). Patients' Personal Data, Including Biometrics, as Objects of Criminal Law Protection. International Journal of Law in Changing World, 1 (2), 46-59. DOI: https://doi.org/10.54934/ijlcw.v1i2.29

[10] Sloot, B. v. (2015). Privacy as Personality Right: Why the ECHR's focus on Ulterior Interest Might Prove Indespensible in the age of 'Big Data'. *Utrecht Journal of International and European Law*, 25-28.

ABOUT THE AUTHOR



Shubham Saurabh
B.A.LL.B. (Hons.), LL.M Candidate at Gujarat National Law University, Gandhinagar
e-mail: shubhamsaurabh668@gmail.com
ORCID ID: https://orcid.org/0009-0003-3060-6580

ABOUT THIS ARTICLE

Conflict of interests: The author declares no conflicting interests.

LA LEY DE PROTECCIÓN DE DATOS PERSONALES DIGITALES DE 2023: FORTALECIENDO LA PRIVACIDAD EN LA ERA DIGITAL

RESUMEN

La Ley de Protección de Datos Personales Digitales de 2023 es una legislación histórica que protege los derechos de privacidad individual y refuerza la seguridad de los datos. Destaca el poder de las personas sobre sus datos personales mediante la introducción de conceptos como el consentimiento, la minimización de datos y el derecho al olvido. La Ley también afecta a las empresas al imponer obligaciones a los controladores y procesadores de datos, exigiéndoles implementar marcos y procedimientos efectivos de protección de datos. La creación de la Junta de Protección de Datos de la India como el organismo central de supervisión será crucial para la aplicación de la Ley. Este trabajo de investigación analiza el poder otorgado a las personas sobre sus datos personales y su impacto en el cumplimiento empresarial, así como los cambios operativos para los controladores de datos, dados los riesgos de sanciones por incumplimiento. El análisis concluye que la Ley de Protección de Datos Personales Digitales de 2023 se erige como un faro para los derechos de privacidad y la protección de datos en el mundo digital.

Palabras clave: datos personales digitales, seguridad de datos, fiduciario de datos, derecho al olvido, consumo de datos

2023年《数字个人数据保护法》：强化数字时代的隐私保护

摘要

《2023年数字个人数据保护法》是一部具有里程碑意义的法律，旨在保障个人隐私权并加强数据安全。通过引入同意、数据最小化和被遗忘权等概念，该法强调个人对其个人数据的掌控权。该法还对企业产生影响，要求数据控制者和处理者履行义务，实施有效的数据保护框架和程序。印度数据保护委员会的设立作为中央监管机构，对于推动该法的实施至关重要。本文研究了该法赋予个人的数据掌控权，以及其对企业合规性和数据控制者运营变革的影响，尤其是在违反规定的处罚风险下。分析得出结论，《2023年数字个人数据保护法》是数字世界中隐私权和数据保护的灯塔。

关键词：数字个人数据、数据安全、数据受托人、被遗忘权、数据使用

https://doi.org/10.54934/ijlcw.v3i2.84