Data Privacy – A Reality That Can Not Be Undermined By the Educational Institutions

Prof. Dr. Md Akbar Khan
Associate Dean, ICFAI Law School, ICFAI Foundation for Higher Education, Hyd

Abstract: **Data processing may include raw data input and conversion to the machine in understandable format, flow of data through the Central Processing Unit and memory to output devices, and formatting or transformation of the resultant output. Data processing could best be described as the utilization of computer technology in order to perform certain tasks on data. Depending on the context and when applied to personal data, "processing" is always a specific operation or a set of operations performed on the data. Such activities include collecting, logging, categorizing, archiving, varying, accessing, utilizing, synchronizing, or integrating data, cataloguing, sharing using transmission, providing access to an individual or making data available to him or her, controlling access, deleting, or obliterating.**

The said judgment was passed on 24 august 2017 by Hon'ble Supreme Court of India. It, without any doubt, held the existence of a right to privacy as an inalienable right to all individuals as protected by the Constitution of India under Article 21. The judgments delivered in case of M. P. Sharma and Kharak Singh were reversed. The said decision enabled the consciousness among the citizens to wake up from slumber to the fact that their privacy might be at risk of being breached during the processing of data of an individual and this decision therefore prepared and challenged the researcher to look for any gaps regarding privacy and protection of data in higher education institutions.

It was nearly six years that the Indian Government took in formulating the Digital Personal Data Protection Act, 2023 and was enacted on the 11th of August, 2023. Before the period of legislation of this law, 21666 suggestions were provided. Now the institutions are in a much better position to protect the data but the odd of escaping has doubled up for them. Data processing has now turned into credibly a work of responsibility and accountability. It has now become imperative for preparation towards protecting and securing the data. The University now cannot afford to take any chances with the data of the students and the staff and would be assuming the role of a data fiduciary and the data processor. As such, it can be posited that data privacy has become a real thing that cannot be dismissed.

Keywords: **Data Processing, Personal Data, Erasure, Breach of Privacy Protection of Data, Data Fiduciary, Data Processor.**

1. INTRODUCTION

1.1. US Scenario of Privacy

The meaning of the term 'Privacy' in Law can be greatly explained by the constitutional provision which defines it as the right of an individual to be left alone. This term, as to its original meaning intended by Michigan Law School's professor Thomas Cooley, refers to protection of personal right to seclusion. From the Pedigree of privacies given by Prof. Allan Westin, it becomes clear that the literal meaning of the term 'Privacy' is 'The state of solitude or small group of intimacy'."

Privacy can be defined as a state or course of action in many ways. This has to do with libelous matters like the diffusion of such detail concerning an illness or a disease, the affairs of a couple on honeymoon, or individual as narrating his authentic private life and intimate relationships, husband-wife domestic relationship, picturing of a moving picture actress taking her bath for some sunbath, bedroom talks, etc. Here, the complaint is not of reputation but of sentiments being outraged. Since the right to privacy means the right not merely to have a right image in private life but actually the right to control the portrayal of private life by others and at times to stop it altogether, the truth could not have been a valid defence in such circumstances The information was provided by one of the panel in 1967 to the office of the US President of Science and Technology.

The right of privacy as stated by Warren-Brandeis and the right to be let alone are the rights of the individual that enable him to choose himself to what extent he will allow others into his inner person, into his thoughts, emotions and details of his life. Thus, men are now all the more inclined to be alarmed. Privacy is an aspect of human nature that prevails despite the ever growing technological roots of society and organizations. There exists life, it is a requirement that is compulsory, still, does that entail compulsory right to privacy? So, the question is: This right must be carried out to reasonable limits, thus,

informing us of the boundaries and extent of this right. Lastly, if this is not the case, what will be the measures taken by us?

By the 1890, Louis D. Brandies and Samuel Warren were fighting for what is called privacy. The U. S. Supreme Court is one of the key players in developing the Fourth Amendment and in protecting it from excessive publicity in recent years. The U. S. Supreme Court did not clearly define the right to privacy of people until 1965, and the only areas it considered it an individual's right was in the aspects of libel and in the Fourth Amendment. The protection of right to privacy under the Constitution revolves around the Fourth Amendment. To begin with, it is crucial to realize that the word 'privacy' is nowhere to be found in the Fourth Amendment or anywhere in the Constitution at all. In fact, as per the Supreme Court, the Fourth Amendment is supposed to be protecting an individual's 'right to privacy' but only up to a 'reasonable level. 'Furthermore, as all known, all searches, including those conducted with a warrant and those conducted without one, must be The Court has stated that in considering the reasonableness of the act of the search, this has to be weighed against the infringing the right to privacy.

In Griswold v. Connecticut [1] the Court sought to intervene for the first time in its modern role with the protection of rights of privacy in connection with marital affairs. However, the court did not elaborate on any specific constitutional right to privacy in relation to marriages. Douglas, J. mentioned that:

Bill of Rights: Zones of Privacy and the Right to privacy; paper also explores the role and contribution of the Bill of Rights' spirit and framework, as well as the sections that made 'zones of privacy', and that the right to privacy existed before the formulation of the Bill of Rights. These arguments awoke an extended sense of construction vend, but, as always, the right genuinely arose from the entire constitutional structure. Germanovsky In addition, it is now conceivable to sue for invasion of privacy as a statutory wrong Pring for trespass or libel or some other tortious legal theory. This has now been sorted out following an extended and strenuous fight with American states. Right to privacy was shifted out from the domain of private law by American courts and shifted to the constitutional law and ensured the protection of this right as part of the public policy. However, this is a legal essays and Griswold cannot be categorically placed in any of the Constitutional Law subtypes. In fact, the Court was almost in some sort of a dilemma on how best to get to a definite Constitutional section, on which to base its judgment. The concept of the right to privacy or the right to be let alone receiving increased attention in recent years, there is a good start here.

It is also within the domain of trade secrets and private directories of economic/commercial relationships that the law of confidence first evolved. It has, however, advanced well beyond this kind of common usage, gaining a foothold in the aficionado technospeak landscape. Before the Courts will order an injunction to keep a secret, three key components must be established:

(a) It must be sensitive to warrant its protection; Compiled records or data for instance are sensitive as they include health details.

(b) The recipient of the information got it from a person who owes the information's owner a duty not to disclose the information.

(c) There are certain things that can be prevented by law so that citizens cannot engage in proposed uses that are incompatible with that duty.

It is possible to illustrate the obligation by linking it to one of the contract members of the families; for instance, the workers might vow not to discuss what they do on the job. People who are involved in the business sector have so much in common despite the fact that some of them have never signed a contract. Some employment relationships, for example, the relationship of a lawyer and his client or a physician and a patient, are intrinsically confidential. Additionally, one should bear in mind that many other third parties who get the information or who must realize that specific information is secret may also have to abide by the condition. Courts have not hesitated to accept the proposition that obligations of confidence may from time be owed to spouses, let alone friends. This means that a newspaper to which a secret is sold or given it can be advised against publishing the same. There is a necessity to recover any other hidden papers that were accidentally shared with a third person. Duty of confidence' as a term is

[1] Griswold v. Connecticut :: 381 U.S. 479 (1965) :: Justia US Supreme Court Center, https://supreme.justia.com/cases/federal/us/381/479/ (last visited May 22, 2024).

used even for a criminal who has stolen personal files of individuals.

1.2. Indian Scenario of Data Privacy Before 2023:

The primary legislation is the Information Technology Act, 2000 while the regulatory rules are referred to as the Sensitive Personal Data or Information Rules.

Another legislation that has to do with the use of Information Technology in India is the Information Technology (Amendment) Act 2008.

Conduct that is Reasonable in Relation to the Sensitive Personal Data or Information Rules, 2011.

subsequently known as the Intermediary Guidelines and Digital Media Ethics Code Rules of 2021.

It is crucial to note that while the cases dealt with the theme of privacy, they failed to acknowledge privacy as a human right.

However, the 8-judge bench of the Supreme Court in the case of M. P. Sharma v. Union of India [2] raised the power of search and seizure where the Constitution framers did not consider that the power of search and seizure confined by any right of privacy. In regard to Kharak Singh [3] the bench comprised of six judges explored on the question of surveillance and regulation's applicability of governing UP police.

The Indian Supreme court validated section 13 defining that the police has the right to carry out domiciliary visits with 'habitual criminals' or those likely to turn criminal and section 17 describing the right to enter and search without a warrant the premises of individuals suspected to be criminals as unconstitutional.

The court, in Govind vs State of Madhya Pradesh [4] upheld the right to privacy but with some restrictions. Even if the fact that this freedom originates from Articles 19 and 21 would be assumed, the Court's decision stated that a fundamental right to privacy could not be absolute, and would only be restricted where the compromise pertains to the compelling public interest test under Article 19(5).

That too in Olga Tellis vs Bombay Municipal Corporation [5] the Indian Supreme Court elaborated the aspect of Article 21 the right to life and liberty and stated that it surpasses the literal animal existence. It postulates more than that, because the guarantee that no one would ever deprive the other of their life means not only the limitations but also the skills that enable one to live as vividly as possible.

One of the earliest and significant cases related to the right to privacy and the right to free speech and expression is the Rajagopal I case in Tamil Nadu (1994) [6]. The libel case was intended for preventing a prisoner, named Shankar and an auto driver from publishing his memoirs.

This means that a citizen has a right to solicit privacy in aspects such as family life, marriage, childbirth and education among other aspects of life. In the case of the book under reference, the state may be allowed to institute a defamation case if any secret contained in the book is bad and an invasion of the state's right to privacy, but the state lacks the powers to prohibit the book's circulation.

Thus the final crux of the matter in analysing the law of privacy'; There is a clear distinction between the physical or bodily privacy and the mental privacy as held in Selvi and others vs State of Karnataka and others [7].

[2] M.P Sharma and others v. Satish Chandra, District Magistrate, https://www.legalserviceindia.com/legal/article-4189-m-p-sharma-and-others-v-s-satish-chandra-district-magistrate.html (last visited May 22, 2024).

[3] Kharak Singh v. State of Uttar Pradesh, https://www.legalserviceindia.com/legal/article-11837-analyzing-the-landmark-case-kharak-singh-v-s-state-of-uttar-pradesh-a-commentary.html (last visited May 22, 2024).

[4] Govind vs State Of Madhya Pradesh & Anr on 18 March, 1975, https://indiankanoon.org/doc/436241/ (last visited May 23, 2024).

[5] Olga Tellis & Ors vs Bombay Municipal Corporation & Ors. Etc on 10 July, 1985, https://indiankanoon.org/doc/709776/ (last visited May 23, 2024).

[6] R. Rajagopal vs State Of T.N on 7 October, 1994, https://indiankanoon.org/doc/501107/ (last visited May 23, 2024).

[7] Selvi & Ors v. State Of Karnataka & Anr, https://indiankanoon.org/doc/338008/ (last visited May 22, 2024).

Three prevalent police interrogation techniques, namely, narcoanalysis, embrace lie detector test and brain mapping or the "Brain Electrical Activation Profile (BEAP) test" were declared by the Hon'ble Supreme Court as unconstitutional prejudicial to the provisions of the rights to life and personal liberty under Article 21 of the Constitution as well as her clauses of Article 20(3) of self-incrimination.

The nine-judge bench of Supreme Court has categorically adjudicated and defined its decision in Justice Adhaar Card case [8] for formalities for the constitutional right of privacy today, it wants to announced that privacy is also a constitutionally protected right occasionally emanating from other aspects of remaining freedom and dignity enshrined and protected under Part III of the Indian Constitution's fundamental rights including Article 21 of the Constitution regarding life and personal liberty.

Speaking of supervision and surveillance, relevant issues related to privacy protection and maintenance should be illustrated in the context of educational institutions. In your view, what strategies are in place for handling the data of the students, teaching, and non-teaching employees in the institutions? Are the institutions erasing their collected data after it has been useful for the goal of its collection or are the institutions holding on to the data much after it has been processed for the intended purpose? How can the data better be protected so that it cannot be captured by hackers, or its security breached or deciphered?

2. RESEARCH OBJECTIVES

- To assess the measures applied in the educational institutions contributing to the protection of students, members of staff and faculty data.
- To investigate the retention period permitted for Data.
- To understand encryption practices being implemented by institutions both globally and at the national level.
- To study the national and international legislative requirements.

3. RESEARCH QUESTIONS

- Whether the weak encryption end up leading to a violation of privacy or violation of Data?
- Whether the weak provisions or no provision of law in the concerned field result in data breaches and violation of privacy.
- Whether the educational institution is erasing data after the purpose is served?
- Who regulates and under what laws at national and international level regarding data protection, specifically the data stored in educational institutions?

4. LITERATURE REVIEW

4.1. Data Protection Laws in India - Everything You Must Know

As stated[9], Data protection is the sum of legal and regulatory provisions and standards that seek to avoid prejudice or violation of privacy by the capturing, storage, and transmitting of personal information. According to specific legislation, personal data is any information or data concerning an identifiable individual immaterial of it being processed by a government authority, a corporation, or an organization.

4.2. The Personal Data Protection Bill, 2019: Key Changes and Analysis

It[10] aims to enhance protection of data privacy in subjects and applies and guides organizations in dealing with personal data.

4.3. Alicia Solow-Niederman, Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches

The paper[11] notes that it is high time the common law was adapted to ensure that the private, personal data is sufficiently protected in case these eventualities, if the issue of information security is to be taken seriously in present day society given the hacks such as Equifax event. This paper aims to point out that if

[8] Supreme Court of India, Justice K.S. Puttaswamy (Retd) vs. Union of India, W.P. (Civil) No 494 of 2012 (2017).

[9] Dr. Ajay Kumar Garg & Shikha Kuchhal, *Data Protection Laws in India: A Comparative Study*, 3 INDIAN J. APPL. RES. 75 (2011).

[10] The Personal Data Protection Bill 2019.

[11] The Yale Law Journal - Forum: Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches, https://www.yalelawjournal.org/forum/beyond-the-privacy-torts (last visited May 22, 2024).

an organisation supposed to be the custodian of an individual's or company's data fails in observing industrial standard and the best practices in terms of operational and security measures then all those updates demand legal action.

4.4. Privacy and Data Protection

The author in[12] also thinks that in the subsequent making of the PDP Bill available for debate and stakeholder feedback, it could be subjected to amendments. The policy decisions concerning data control and sharing, particularly data transfer across borders, will impact a bulk of Indian companies.

5. METHODOLOGY AND DATA SOURCE

The present study is doctrinal. In the doctrinal study, the legal provisions are analysed and interpreted to reach a conclusion. The secondary data has been sourced from Text, Reference Book, journals, magazines, newspapers, articles, Information retrieved from the Government Departments, Organizational records & the Websites.

6. INTERNATIONAL LEGAL FRAMEWORK

6.1. United Kingdom- Data Protection Act

EU General Data Protection Regulation 2016/679 known as the GDPR;

Specifically, this paper's scope of consideration is the Privacy and Electronic Communications (EC Directive) Regulations 2003, also known as the E-Privacy Regulations.

According to the Data Protection Act of 1998 playing the role of an information controller it is the responsibility of a person to ensure that proper handling of information is done and this is done through compliance with certain eight principles.

The data must be:

• Aimed for a limited purpose and still conducted in a legal and lawful manner.

• only that which is important for the function, the necessary and sufficient amount of information and not abundant.

• accurate;

• adapted and not stored for more than is necessary to achieve the organization's goals;

• collected, used, and retained in line with the lawful data processing requirements for the data principal;

• secure; and

• have not been transferred to other nations, without adequate protection for such transfers and for the consent of the people involved.

The data fiduciary must meet certain six conditions when such information can be considered processed if for the information is personal data related to a living individual who can be identified from the information or the information at the possession of or likely to be in the possession of the data controller or the data fiduciary.

The following scenarios apply to data processing: The following scenarios apply to data processing:

1. Either the consent of the data subject or the data principal has been received;

2. The processing is needful to fulfil a contractual obligation to which the data subject, or the data principal, is a party to.

3. The processing is necessary in order to fulfil a legal or regulatory requirement which the data fiduciary is bound by but which does not arise from the processing undertaken at the instance of the former;

4. The processing is to fulfil the obligation that is of significance to the data subject's vital interest.

5. Processing is necessary for the performance of state functions or the administration of justice purposes.

6. The processing is necessary for the purposes of pursuing the legitimate interest of the data fiduciary the third party, or other parties to whom the data are disclosed; otherwise, the processing does not seem reasonable because it will impact the rights, freedoms or legitimate interests of the data principal.

Where the information concerned involves special category personal data as defined under the Data

[12] (PDF) 'Privacy and Data Protection Laws in India: A Right-Based Analysis, https://www.researchgate.net/publication/323958405_%27Privacy_and_Data_Protection_Laws_in_India_A_Right-Based_Analysis (last visited Sep 21, 2023).

Protection Act of 1998, one of several additional conditions must be fulfilled. These conditions include:

The five modes are: (a) Processing information with the consent of the subject;

(b) To process information for the purpose of employment as required by law;

(c) Processing information required in the legitimate interest of the subject or another person in order to protect the vital interest of the subject or of another natural person.

Some of the tasks that can result in a failure to discharge one's duties appropriately in relation to the administration of justice or the handling of legal proceedings include:

The following categories of personal information are considered to be sensitive personal data: The following categories of personal information are considered to be sensitive personal data:

1. Basic data or data primary that is the race or ethnic background of the data subject;

2. His views on politics;

3. They may have frankly denied or at least not approved of his religious beliefs or any other similar phenomena.

4. physical or psychological condition of the individual,

5. His erotic pursuits;

6. The offense that he has committed or is believed to have the offense that he has committed or believed to be committed.

7. Everything concerning the performance of any action related to any crime he may have probably perpetrated or is in the middle of perpetrating, the end product of which; or the outcome of the actions as determined in a court of law.

6.2. European Union- General Data Protection Regulation (GDPR)

Author would like to specify that European countries are the only regions that have a well-developed data protection strategy. This is true now more than ever given that the advent of the widely implemented and recognized regional treaty known as the European General Data Protection Regulation (GDPR) was implemented in May 2018. [13]. In 2018 GDPR, the EU's new data protection legislation has the same aim as the 1995 Data Protection Directive: to achieve a consistent level of safeguarding individuals' rights and freedoms in their processing data and in the free movement of this data within the EU Members States. Article 5 [14] of the regulation, enshrines seven key criteria for the lawful handling of personal data, namely: Legal, justified, and transparent; use limitation; data minimization; data accuracy; retention purpose; data integrity (security) and confidentiality; responsibility. Obedience to these principles, in their truest form becomes the essential basic/common element for the practice of good data protection. It is in 2018, GDPR of Europe introduced new rules with regard to an individual's right to his data and the bar of digital privacy has been created. The principle of GDPR in the aspects of the customers is the corporate-customer-relationship where GDPR intends to give clients more influence on the purchasing or obtaining of their personal data. Fines could be imposed in case of violation of the provisions of the Act. It is imperative that organizations that fail to meet the requirements of GDPR should be liable for a fine higher than that of EU 20 million or 4% of their annual turnover globally. Thus one can observe that the recent regulations coming out of the EU are being met with serious consideration. GDPR's main objective is to help protect clients from businesses that are not following all the necessary privacy requirements. In the EU, the company that has direct access to customers' data and processes it on behalf of the business is referred to as a data processor. After adoption of GDPR, people enjoy the right to request the information that is kept in the databases of various corporations, and corporations, in turn, have a set of rights and obligations related to the proper handling of the data within their jurisdictions as well as to face a new system of fines upon violation.

[13] General Data Protection Regulation (GDPR) – Legal Text, https://gdpr-info.eu/ (last visited May 22, 2024).

[14] *Id.*

6.3. GDPR (Article 5(1)) presents six privacy principles they are

- Transparency, Fairness, Lawfulness.
- Restrictions on the processing, storage, and purposeful gathering of data.
- Minimizing data
- Data integrity and secrecy;
- Limitations on data storage; and
- Data accuracy.

7. NATIONAL LEGAL FRAMEWORK

This decision is known as Puttaswamy judgement given by Supreme Court of India which brought the concept of 'Privacy' under the realm of Right to Life and Liberty and included it in the Article 21 of Indian Constitution which paved the way to enact a single statute for Data protection in India. In the Puttaswamy Judgement, rights of private individuals are highlighted and the scope of rights of the Citizen has been emphasized rather than the rights of the State. "The Supreme Court identified the value of privacy with the value of personal dignity; and relying on common-law authorities pointed out that the State had a positive duty to respect this dignity," This means that through the Puttaswamy Judgment, both privacy invasion by the State and invasion of privacy by individuals, contracts and exchange of information are prevented because it declares that it is the responsibility the State to regulate such issues to protect the dignity of an individual.

Therefore, the Sri Krishna Committee was formed; and in 2018 the Draught Personal Data Protection bill was issued. The bill was introduced in the Rajya Sabha in December 2019 after the Ministry of Electronics and Information Technology made changes to the draft based on criticisms from different stakeholders and industries that dealt with the previous text of the PDPB.

The PDPB, thus following its guiding principles, has called for changes in India's legal provisions governing data sharing contracts in business. of measures taken until now, it has provided high penalties for noncompliance; set strict compliance obligations for all categories of PDP; extended the rights of the data subjects; appointed the single national body regulating data protection; and initiated the localization rules for specific types of sensitive data.

Though, several issues related to its implementation have emerged, and these led to the JPC scrutinizing the PDPB in 2019. THE JPC then left the public to guess until it again delayed the review and debate of the taps and tweaks of the PDPB for about 2 years, and all the while the world was coping with a pandemic.

The government of India in July 2020 released a consultation paper on new framework guidelines for the management of NPD touching details of its governance – the NPD Report. Based on the analysis of subcategories, related objectives, and driven by the need for changing the context of NPD and its evaluation, the NPD Report was developed to define legal, economic, social, and commercial value of NDP for corporations, startups, and the government. In the NPD Report, over 1,500 responses were received by the committee wherein; based on the feedback, changes were made. Some of the tentative policies and frameworks became refined, namely, the PDPB and the Non-Personal Data Governance Framework; their scope and the purpose of cross-border exchange of the NPD were narrowed down by the same committee in the revised NPD Report in January of 2021.

Later in November of 2021, the JPC has forwarded its report incorporating the changes and the draught of the legislation. The new name of the PDPB is the Data Protection Bill 2021 ("DPB") which had some changes from the preexisting versions. It was a great improvement to see that law was made for data personal and non-personal both. This is due to the stringent reporting procedures for data breaches adopted by the PDPB, a rule in the hardware manufacturing sector, the provision of an accreditation framework to certify all digital and IOT devices, and the PDPB's requirement for an extra measure of data compliance needed for consultation with the Central Government where there are transfers of special personal data and critical data. The DPB also provided for phased implementation, and although the deadlines mentioned were to be complied with at the end of March of a specified year, the Central Government might select different dates for the incorporation of some key clauses.

Originally, the PDPB was planned to be presented to the Parliament in the session that occurred in February 2022, but the new version of the law was rather poorly received, and numerous stakeholders, including JPC members and representatives of domestic and foreign business, as well as various circles, criticized it for a number of reasons, one of the most significant of them being the fact that, as

compared to the foreign equivalents, the PDPB focused upon safeguarding state interests than private individuals data privacy.

The poor of developing nations are also unsure of PDPB in the future. Many print, electronic, and online media have also reiterated that the Indian government has withdrawn the PDPB in order to adopt new budding data protection regulations. It might also be prospective to amend the IT Act in a way that addresses the requirements of the developing technological environment in the nation, as sources suggest.

The Ministry of Electronics and IT (MEITY), in February 2022, unveiled India's Data Accessibility and Usage legislation/Data Usage Policy to harness the value of public sector data given the unpredictability of India's implementing legislation on data security. It can also complement policy, if needed, to address current challenges to data access while accepting open data as a valuable public asset. Open data can be defined as any data or information which is freely usable, available, and redistributable which is set by Indian Government policies that cover every data and information produced, collected, developed or maintained directly or indirectly by various ministries, departments, organization, agencies, or autonomous bodies.

Policy is beneficial in making visible the potential monetary worth of data within the public domain, and it may make possible the sharing of the desirable data to foster advantage in the business environment. As from practical experience it becomes challenging to apportion causation and remedy for violations of right to privacy or data leakage owing to the fact that there is no well-structured law of privacy and data protection in India nor is there adequate structural unity.

It currently seems that India's five-year long endeavour to impose stringent data protection and privacy standards has fallen within the short-term. However, in the light of actions taken by the Indian government about the controversy related to the reform of the IT Act as well as about the framework for exchanging data in PSU, comprehensive data governance architecture for India will be developed in the next couple of months. That is why it would be intriguing to see how the data protection system changes and is reshaped in some way; this would be stimulating and would require active interference from PBBs.

A complete law protecting the data and regulating the data would definitely have effect on and will certainly enhance the formulating of the global data governance atmosphere as India is one of the biggest data markets internationally. This was done after the cabinet passed the Digital Personal Data Protection Bill, 2023, which after passing in both the houses of the parliament on August 7 and August 9, respectively got the president's assent on August 9, 2023 and came to be an Act on the August 11 and became a member of nations with data privacy laws.

8. ADOPTION OF PRIVACY PRINCIPLES IN EDUCATIONAL INSTITUTIONS

GDPR (Article 5(1)) presents six privacy principles they are

- Transparency, Fairness, Lawfulness.
- Restrictions on the processing, storage, and purposeful gathering of data.
- Minimizing data
- Data integrity and secrecy;
- Limitations on data storage; and
- Data accuracy.

Fundamentally, the Educational Institutions need to obtain the data from the student, faculty & staff in compliance with the Article 5(1). In the course of the study the educational institutions have been using the centralized server and all the data collected for research are saved in an unencrypted format. The data thus collected is prone to mini vulnerabilities like the data being processed by third parties, sometimes the third parties processing the data may be accessing personal sensitive data hence compromising the data, again the data lacks proper protection mechanisms in place sometimes it is easily hacked and identity theft may occur.

The educational institution from-

Student- Certificates required for verification- Qualifying certificates, Aadhaar information, Migration certificate, social status, Income details of the family for the annual income, Medical details.

Faculties – Residence details, Bank details, Academic certificates- these details should include the PAN card number, Aadhar number, and house address.

Staff- House address, Bank Account number- A/C no., Qualification details- education, PAN card, Aadhar card.

1. Legality and Proportionality-

According to the legal authorities and rules and regulation of university, the admin department needed to obtain the aforesaid detail for payment of the salary, remuneration, and performance. This must be followed by legal basement for collection of information. It must be in proportion to the needs of processing and so be more discreet and less obtrusive.

Student data are gathered to process those who applied, for rewarding, and awarding of degree and scholarship. The criteria employment of this Aadhar information is not mandatory in the case of any private organization or at the time of admission as mentioned in the Aadhar Act 2017. Aadhar information can only be disclosed when someone wishes to take the benefit through any authorities either government or other.

2. Purpose Limitation-

The information that will be collected from the various concerned parties and stakeholders should also be collated and kept safely in the institution servers. The following are important points used when storing information: The information so stored must be relevant to the purpose for which it is collected. The need information should be in harmony with the laid purpose served.

3. Data Limitation-

The collected data should be proportional to the volume required for the purposes of collection and processing. The purpose for which the institutions have been collecting data rules out any possibility of collecting other types of data which are unnecessary or surplus.

4. Correctness of data-

Information may also have to be updated at regular intervals by the educational institutions in order to maintain a record of the updated information and data, and the data has also to be made available to the stakeholders to update it. In failure to do so, such data will be completely misleading, and the information gathered so far will eventually turn out to be completely useless.

5. Data retention limits-

These days, institution is using cloud storage as an archive location for the information it contains. It can be easily accessed and can be accessed from anywhere which makes it far more safe and secure as opposed to conventional storage.

6. Transparency, Accountability, and Confidentiality-

Personal information collected from educational institutions must be kept secret, and preventive steps must be taken to make some information difficult or impossible to decipher for intruders to gain access to it and infringe on the privacy of individuals. The organization's authorities should process the information and not allow the third party or other organizations that may lead to compromise of privacy, transparency, accountability, and confidentiality.

9. SUGGESTION/RECOMMENDATION

The importance of improving security and privacy protection through encryptions should be enhanced in educational institutions. Thus, according to the requirements, cryptographic methods that can be applied are standardized ones, including the usage of symmetric and asymmetric encryption.

- Develop the rules and requirements for the data-gathering process in the educational context to determine which data can be gathered from learners as well as employees and which is irrelevant.
- Establish a grievance cell for the complaint process for privacy and data-related concerns of students and staff members. This cell should comprise main stakeholders from the student community, faculty, other teaching and non-teaching staff, and the management sectors of the organization.
- Each member in the grievance cell should specialize in data protection and security and be capable of handling the aforementioned issues.
- At the department level, departmental heads should ensure that they have complied with all the set standards on data collection.
- At the university level, the registrar should take the mantle of data protection to ensure that the university adheres to the rules and regulations set regarding data collection.
- Privacy measures can thus be improved by letting the Data Protection Authority conduct periodical checks on the organizations.

10. CONCLUSION

Namely, the user specifies the areas where students and staff in educational facilities should be protected

from data breaches. Stakeholder studies reveal that there is limited information about the privacy issues and confidentiality measures that are being undertaken in the course of implementing e-learning. Besides, many participants do not know the safety procedures, either, 27% of participants stated that they do not know the matter of concerning encryption techniques.

They have also complained of the inability to access and change their data as the situation has often been presented. In this regard, previous studies have found that institutional systems hold more information than actual requirements, and, more often, the data is not deleted even when it is no longer helpful to the target user.

There are also still doubts about current data protection laws. Many people still expect the new data protection law, the Digital Personal Data Protection Bill 2022, to be in high demand, and the public has provided 21666 comments to the Ministry of Electronics and Information Technology. These concerns were obtained after a public consultation was sought when the bill draft was published in November 2022.

The Bill has been termed the Digital Personal Data Protection Bill 2023 and was approved by the present cabinet on the 5th of July, 2023. It was tabled in the parliament during the monsoon session that began on the 20th of July, 2023.

The Digital Personal Data Protection Bill,2023, with 21,666 suggestions, was finally passed in Lok Sabha on the 7th of August, in Rajya Sabha on the 9th of August, and the President granted assent on the 11th of August,2023.

Now, we have an act that will be a game changer and is expected to uphold the sanctity of every citizen's fundamental 'right to data privacy' in real and virtual realms. Nevertheless, the rules are framed but still to be implemented, so the law awaits enforcement.

REFERENCES

[1] Practical Guide to Digital Personal Dat Protection Act,2023 Law and Compliance, Puneet Bhasin,OakBridge(2024)

[2] Taxmann's Digital Personal Data Protection Act 2023 [Bare Act] – Covering amended & updated text of the DPDP Act along with FAQs on various topics [2023 Edition] by Taxmann

[3] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 with Gazette Notifications, Press Release, Comments, Short Notes & Caselaw by Rajan Nijhawan -- 1st Edition 2021

[4] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 with Gazette Notifications, Press Release, Comments, Short Notes & Caselaw -- 1st Edition

[5] Data protection law and regulation paperback – 2019 by Apurv sardeshmukh (author) Publisher: Thomson Reuters (2019)

[6] Data Protection Laws Demystified [Print Replica] Kindle Edition by Amar K Sundram Anghrija Chakraborty, Ashima Obhan (Author) Publisher: OakBridge; 1 edition (10 October 2019)

[7] Cyber Forensics in India: A Legal Perspective Hardcover – 1 Mar 2017 by Nishesh Sharma (Author) Publisher: Universal Law Publishing - an imprint of LexisNexis; First 2017 edition (1 March 2017)

[8] Gerald Spindler and Fritji of Bomer: E Commerce Law in Europe and the USA, Published by Springer-Verlag Berlin Heidelberg, Edn. 2002

[9] Alam Davidson: The Law of Electronic Commerce, Cambridge University Press, South Asian Edn, 2011.

[10] Garima Tiwari: Understanding Laws, Cyber Laws and Cyber Crimes, Lexis Nexis, 2014

[11] Henry R: Contemporary Business Law and On-Line Commerce Law, Prentice Hall, Inc. 6th Edition, 2009

[12] Andrew Grant Adamson: Cyber Crime Mason Crest Publishers, Edn 2003–

[13] Jain NC: Cyber Crime, Allahabad Law Agency, Edn, 2008

[14] Nina Godbole, Sumit Belapure: Cyber Security, Wiley India Publishers (Kindle Edition), 2011

[15] Aparna Vishwanathan: Cyber Law –Indian and International Perspectives on key topics including Data Security, E-commerce, Cloud Computing and Cyber Crimes. Lexis Nexis, Butterworths Wadhwa, 2012.

[16] Barkha&U.Rama Mohan- Cyber Law and Crimes, Asia Law House, 3rd Edn 2011.

[17] Bansal S K: Cyber Crimes, published by Aph Publishing Corporation, Edn 2017.

[18] Edward Amoroso: Cyber Security, Kindle Edition, Silicon Press, Edn 2006)
[19] Brijendra Singh: Network Security and Management, Kindle Edition, PHI, 3rdEdn 2012.
[20] Henry R Cheesman: Contemporary Business and E-Commerce Law, Prentice Hall; 4 Edition 2002.
[21] Dr. Dasgupta: Cyber Crime in India: A Comparative Study, Eastern Law House, 2014.