Innovations

Data security and Digital data protection with reference to the Digital Data Protection Bill 2022

Dr. Sunita Arya
Principal, Department of Law, Prestige Institute of Management and Research, Indore
Kusum Joshi,
Assistant Professor, Indore Institute of Law, Indore

*Corresponding author: **Dr. Sunita Arya**

Abstract:
The growing population implies growing interactions with digital devices and the internet, consequently resulting in a humongous amount of generated digital data by the users. This data, which is largely available on the internet, can be effectively accessed and used by the mega-companies or organizations which are referred to as "data fiduciaries" sometimes even without intimidating the data privacy and infringing their Right to Privacy which is a fundamental right under Article 21 of the constitution. These data fiduciaries are generally very strong and have unbridled bargaining powers as they, up to an extent, influence the economy and politics of a country[1]. Nowadays, data is crucial in information combat. Data is a necessary component of Artificial Intelligence. As a consequence of digital revolutions, the amount of data about an individual is expanding[2].

Keywords: *1.Data privacy, 2.data security, 3.data protection, 4.data security controls, 5.cyber security, 6.data fiduciaries, 7.the Digital Data Protection Bill 2022*

Introduction:

Digital privacy refers to the protection of an individual's information that is used or created while using the Internet on a computer or personal device. India, for long, has struggled to table a nearly flawless and uncontroversial law on privacy. The present legal framework which primarily governs privacy under the Information Technology Act (IT Act), 2000, and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (IT Rules), 2011 nearly fails to keep up with the technological advancements and the growing exigency to have a proper data protection law. Thus, the need to enact an unblemished law on privacy and data protection in India is undisputed[3].

Importance of Data Security

Data security is the practice of protecting digital information from unauthorized access, corruption, or theft throughout its entire lifecycle. It's a concept that encompasses every aspect of information security from the physical security of hardware and storage devices to administrative and access controls, as well as the logical security of software applications. It also includes organizational policies and procedures. When properly implemented, robust data security strategies will protect an organization's information assets against cybercriminal activities, but they also guard against insider threats and human error, which remains among

the leading causes of data breaches today. Data security involves deploying tools and technologies that enhance the organization's visibility into where its critical data resides and how it is used. Ideally, these tools should be able to apply protections like encryption, data masking, and redaction of sensitive files, and should automate reporting to streamline audits and adhering to regulatory requirements[4].
Protecting data from internal or external corruption and illegal access protects a company from financial loss, reputational harm, consumer trust degradation, and brand erosion. Furthermore, regulations for securing data, imposed by the government and the industry, make it critical for a company to achieve and maintain compliance wherever it does business[5].

Main elements of Data Security[6]

The three components of Data Security that all companies should adhere to are confidentiality, integrity, and availability. The CIA triad is a security paradigm and framework for the protection of data. Here is what each fundamental piece implies in terms of preventing unwanted access and data ex-filtration.

- **Confidentiality:** Ensures that only authorized users, with appropriate credentials, have access to data.
- **Integrity:** Ensures that all data is accurate, trustworthy, and not prone to unjustified changes.
- **Availability:** Ensures that data is accessible and available for ongoing business needs in a timely and secure manner.

Types of Data Security Controls[7]

- **Access Control**
  Limiting both physical and digital access to central systems and data is an example of a strategy for securing data. It involves ensuring that all computers and gadgets are password-protected and that physical places are only accessible to authorized employees.
- **Authentication**
  Provide authentication measures, such as access restrictions and correct identification of people, before giving access to data. Passwords, PINs, security tokens, swipe cards, and biometrics are common examples.
- **Backups and Disaster Recovery**
  Good security means you have a strategy in place to safely access data in case of a system failure, disaster, data corruption, or breach. To restore, you will need a backup data copy kept on a distinct format such as a hard drive, local network, or Cloud.
- **Data Erasure**
  Appropriate discarding of data regularly is necessary. Data erasure is more secure than ordinary data wiping since data erasure uses software to wipe data completely on any storage device. Data erasure or Data Wiping ensures that data cannot be recovered and, hence, will not fall into the wrong hands.
- **Data Masking**
  Data masking software obscures letters and numbers with proxy characters, concealing information. Even if a person obtains access to data illegally, it is successfully masked. Only when an authorized user acquires data, only then it reverts back to its original state.
- **Data Resilience**
  With comprehensive security, you can withstand or recover from failures. Avoid power outages and mitigate natural catastrophes as these factors can breach data protection. Data privacy can be implemented by incorporating resilience into your hardware and software.
- **Encryption**
  With the help of encryption keys, a computer algorithm converts text characters into an unreadable format. The content can only be unlocked and accessed by authorized people who have the

appropriate keys. To some extent, everything from files and databases to email conversations should be secured.

Data Security is now a must-have, and the importance of data security is increasing day by day, hence the financial investments that your company is willing to make should reflect that. Your investment must be comprehensive and continuous throughout. You must provide protection and the best guidance and training for your employees. One error is sufficient to bring down an entire network. To avoid this, keep your employees trained. It is easier to perceive tighter data restrictions as a means to protect your business. Your team will be limited to providing services to clients if there is no access to significant insights of data.

Key data protection suggestions[9]:

1. Use strong encryption

The days are long gone when strong encryption was only needed for the most sensitive data. Now, it should be standard practice for any kind of personal information. Make sure that both at-rest data, such as that stored on physical servers, and in-transit data, including information transmitted to and from cloud services, are covered. Among the most crucial data protection tips is to look for an algorithm such as Advanced Encryption Standard (AES) that offers at least 128-bit encryption; 256-bit encryption may be appropriate for very sensitive data. Using HTTPS web connections adds a useful extra layer of security.

2. Prioritise staff training

Even one weak link in a chain can make it vulnerable, so investment in your staff is vital. All managers and other employees need to know what's expected of them in any particular situation, and how to practice good data security as a matter of course. Emphasize the need for discretion in communications, never including personal details in emails unless this can be fully justified. Ensure that staff access to systems containing personal data is limited to areas directly related to their professional activities, and underline the importance of recognizing false requests for information.

3. Minimise data use

In terms of both data capture and data consumption, use only that personal information which is necessary. Profiling for marketing use may be unavoidable, but best-practice data protection tips include remembering that it may be just as effective when psuedonymised. Certain fields, such as people's titles, are often not needed at all. When it comes to consumption, only request data from customers that is needed – if someone simply needs to be over 18 to access a certain service, that's all that matters. There is no need to ask whether they're 32 or 33, or what level of educational study they attained.

4. Store data no longer than necessary

Holding onto personal data you don't actually need is poor practice and may in some cases fall foul of legislation like the UK Data Protection Act or the more recent **GDPR**. Also, bear in mind that much personal information evolves and changes as time goes on – home addresses and mobile phone numbers, for example. Among the data protection tips that is often forgotten is to limit the time data can be stored before asking customers to re-confirm and update details as well as reassuring them that they remain in control of how their data is used. Strengthening trust with customers also makes them more likely to choose you in the future.

5. Ensure crisis resilience

While nobody likes to think about the possibility of a major disaster striking the business, there are many ways this can happen, ranging from flooding to fires. Consider how you would deal with such a crisis, and

how to avoid crucial data being lost in such circumstances. Under the Data Protection Act, you must have adequate safeguards in place to guard against loss from accidental damage. Digital documents stored on a secure cloud server can be easily and swiftly restored once the company is up and running again.

6. Manage passwords properly

Without strong password protection, you may as well be leaving the door of your virtual office open to anyone who wants to walk in, and this forms another of the most crucial data protection tips. Effective password policies are critical for every business. Ensure that passwords are required to be changed regularly, such as every 90 days, and that old passwords cannot be reused. Guard against staff falling back on insecure options such as basing their passwords on their names, company positions or other easy-to-guess terms. Audit password changes to allow you to keep track of when they change – this will also help to solve password security breaches.

7. Invest in a visitor management solution

Keeping your visitors safe and secure becomes simpler and more straightforward with an effective and coherent visitor management solution. This makes sure that your organization is resistant to unauthorized intrusions, whether as a result of industrial espionage, drive-by attacks or opportunistic data theft. This tip for protecting your data also brings benefits for genuine visitors in making them feel welcomed and their needs understood.

The Digital Data Protection Bill 2022[8]

The Personal Data Protection Bill 2021, proposes a comprehensive data protection regime while easing restrictions on non-personal data collection and cross-border data transfers. While the new bill is more amenable to businesses in the country, it also levies hefty fines for non-compliance, a clear indicator that organisations need to buckle up and formulate data privacy programs now. Currently, data protection in India is governed by the Security Practices and Procedures and Sensitive Personal Data or Information, 2011 and the Information Technology (Amendments) Act, 2008. But the Digital Data Protection Bill, once enacted, will have significant implications for virtually all organizations operating in India. Many companies will be challenged with transitioning from complying with SPDI Rules to the new and more complex law.

Step 1: Maintaining a defensible data inventory

If you don't know where your data lives, who has access to it, and who in your organization is responsible for it, it becomes impossible to comply with regulatory mechanisms. For instance, the Digital Data Protection Bill calls for "every data fiduciary (businesses) to have in place a procedure and effective mechanisms to redress the grievances of data principles (its customers)."

For organizations to effectively address the grievances related to customer data, they must have an effective inventory of data that resides across departments, in one centralized repository. This is next to impossible for organizations with large amounts of data without the right technology to ease processes. More importantly, because of the growth in the amount of data held over the last years, the problem gets worse if the data is not inventoried. With tools that are easy to configure and scale, organizations can create a legally-defensible data inventory that provides a roadmap to meet compliance obligations, identify existing vulnerabilities, and demonstrate accountability.

Step 2: Manage data subject access requests

The Digital Data Protection Bill fleshes out specific rights of customers to access information about their personal data. In addition, the legislation calls for organizations to have data pertaining to each subject in one place as each individual is entitled to receive a "summary of the personal data that has been processed by the data fiduciary and with whom the personal data has been shared along with all categories." Without a defensible

data inventory, such subject access requests would take an inordinate amount of time to process, which would be in direct violation of the law.

This is why businesses in India need a robust system that can handle the intake of the request, verify the individual or entity's ID accurately, and also collect, review, and redact necessary information. Since the new legislation governs employee data too, businesses require tech stacks that can access employee data, requiring integrations with HR systems to ensure that employee records are correctly retained. When technology harmonizes data deletion requests with other legal obligations and compliance mechanisms, the process becomes easier.

For instance, the proposed bill gives individuals the right to request deletion of their personal data in possession of an organization 'X'. 'X' is required to identify the data and delete it and this would take massive amounts of time if done manually. The organization would have to source information residing across departments, check with legal departments on whether or not other compliance mechanisms require them to retain data and then delete the data. But an automated tool can accurately process such requests in a matter of minutes.

Step 3: Manage third-party risks

The new data protection bill proposes a hefty fine of Rs 250 crore to "take reasonable safeguards to prevent personal data breach". As data volumes explode, so do organizations' responsibility to safeguard customer data. With cyber crime increasing year on year, it is not unfounded that regulatory mechanisms require organizations to take measures to protect the privacy of its customers.

When we look at how organizations are handling cyber security regulations, there's typically one area that drives a lot of risk: third parties. More specifically the gap in visibility into third-party activities — which vendors have access to organizational data — and which of those are risks that need to be contained to comply with the upcoming privacy regime?

Let's simplify this further. About 65% of successful organizations have outsourced operations to some capacity and a vast majority of them have migrated to the cloud. Cloud solutions often connect to other data sources within a business. This means that your critical business data and your customers' personal information is likely to be accessed by third party vendors. For organizations to be truly compliant with the upcoming legislation, they need to fill a lot of gaps in knowledge about what customer data third parties are accessing and whether it is being done securely. With the right technology, businesses can assess and capture details about vendors to ensure compliance frameworks aren't compromised.

Step 4: Data retention and minimization

While data minimization is a great way to establish deterrence against cyber attacks, the reality is that most organizations retain data longer than they need to. The new data protection bill addressed this issue and specifies that businesses only need to retain the data they need. "A data fiduciary must cease to retain personal data when the purpose of such personal data no longer serves the purpose for which it was collected." But the bill also makes exemptions for businesses that are required to retain data like banks, which are mandated to retain data for six months.

Data minimization is great in reducing legal and cyber risks. Data you don't keep can't be breached when subject to a discovery request. This means that keeping only the data that is important to essential business practices will mitigate risks from litigation and data privacy regulations.

But with so much data and multiple regulatory norms that govern it, organizations may find themselves at crossroads on whether or not they need to retain disparate sets of data they have. With the right tools, data minimizations can be a simple process as it can identify which data is under another regulatory obligation — like a legal hold. Technology can bring about a harmony between data minimization and retention, all while ensuring organizations stay legally compliant.

A changing legal world requires technology that stays up-to-date, and all compliance needs pertaining to data privacy and protection are met. If businesses in India don't begin implementing effective data protection

programs now, they will have to play catch-up once the new legislation is enacted. Overhauling existing processes can seem arduous but with the right tools, businesses can streamline privacy-related issues and also stay ahead of the game by ensuring their processes are adaptable and scalable.

Conclusion

An estimated 137 out of 194 countries have put in place legislation to secure the protection of data and privacy, with Africa and Asia showing 61% (33 countries out of 54) and 57% adoption respectively, according to data from the United Nations Conference on Trade and Development (UNCTAD), an intergovernmental organization within the United Nations Secretariat. Only 48% of Least Developed Countries (22 out of 46) have data protection and privacy laws.

References

1. *www.livelaw.in*
2. *www.expresscomputer.in*
3. *www.livelaw.in*
4. *www.ibm.com*
5. *intellipaat.com*
6. *Ibid*
7. *Ibid*
8. *www.visipoint.net*
9. *timesofindia.indiatimes.com*

*Corresponding Email id: ***dr.sunitaarya@yahoo.com kusumjoshi1828@gmail.com***