A March towards Digitization

1. Introduction

Digitalization, a moving wagon in which every individual and body corporate[1] has stepped in to make their wagon a battery-operated supercar wherein everyone now wants a Tesla. Digitalization is a positive step taken by government of India enhancing effectiveness of doing business i.e. from online filings, banking to insertion of digital signatures. On the flip side, it has an array of problems including breach of personal data, confidential information and over dependence on the internet. While data protection is a concern for individuals and corporations, intermediaries receiving data need to assess their obligations, liability and the content of information posted online in conducting business.

This newsletter provides a high-level overview of selective provisions of technology laws followed by corporate bodies and intermediaries and the issues faced while complying with such laws.

2. Legal Framework

2.1 Data Protection

The legal framework is covered in the Information Technology Act, 2000 ("**IT Act**") and Information Technology (Reasonable Security Practises and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**Data Rules**"). The IT Act mandates body corporates to protect data[2] and any sensitive personal information; for example, passwords, financial information, medical records, etc which should be handled with reasonable security practises. Rules 3 through 8 contain express provisions on how the data should be handled.

Any entity dealing with data has to necessarily **(a)** publish a privacy policy[3] on its website for users with details about the treatment of information provided by users availing services of a body corporate; and **(b)** secure consent of the information provider before transfer or disclosure of sensitive personal data. Pursuant to Rule 5 of the Data Rules, while securing the consent, the body corporate has to provide details about its usage, so that the data giver is secure and satisfied that its data shall not be abused. It is also important that the information collected is for a lawful purpose, retained for the time period it is required and allows the provider to rectify and retract their information at any point in time.

Disclosure and transfer of information provided under Rule 6 and 7 **(a)** mandates prior permission from the data giver under a lawful contract (or otherwise) except when required to be shared with government agencies, or where disclosure is essential to comply with a legal obligation; and **(b)** prohibit data sharing with any third party, but may be transferred to an entity

1 Section 43A of IT Act defines body corporate as a company which includes a firm, sole proprietorship or association of individuals. In this newsletter it is used interchangeably with corporate bodies and entities
2 Section 2(1)(o) defines data to mean representation of information, knowledge, facts, etc. processed in computer system in any form or stored in its internal memory
3 See Rule 4 which contains details on the content of such policy

under a contract or with a prior consent, provided such third party adheres to the same degree of protection as covered under the Data Rules. Every entity has an obligation to implement reasonable security practices and procedures to protect data from unauthorized access, use and damage. Reasonable security practices means having a comprehensive security programme in place which consists of security measures including managerial, technical, operational and physical that commensurate with the information in order to safeguard and prevent breach. IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System - Requirements" is a globally accepted standard. Alternatively, organizations can follow best code practices approved by government of India.

For failure to ensure data protection through maintaining reasonable security practises, privacy and confidentiality, IT Act provides **(a)** corporate body to pay damages to the affected person[4]; and **(b)** data disclosed without consent shall hold the disclosing party to be punished with imprisonment of three (3) years and/or fine of INR 500,000[5] (about USD 8,000)[6].

2.2 Intermediaries Guidelines

An intermediary is defined under section 2(1)(w) of the IT Act as any person, who receives, stores, transmits electronic record or provides services from such electronic record. To regulate conduct of intermediaries, specific rules were notified as Information Technology (Intermediaries Guidelines) Rules, 2011 ("**Intermediary Rules**") which essentially contain only 3 Rules, but with stringent obligations. Entities collecting data electronically such as Airtel, Facebook, Amazon, PayTM, Google, etc. qualify as intermediaries. The challenge remains since both the intermediaries as well as users[7] are unable to unequivocally understand their respective duties and rights.

There is an overarching obligation on every intermediary to be diligent in the discharge of its duties under Rule 3 of the Intermediary Rules. Such duties include publishing rules and regulations, privacy policy and user agreement for accessing intermediary's computer resource and informing users not to share information which **(a)** harms others (i.e. defamatory, obscene, contains virus, etc.); **(b)** infringes intellectual property; **(c)** violates any law; or **(d)** threatens Indian sovereignty[8], etc.

Once the intermediary is aware that prohibited information is hosted on its website, it must take action within thirty-six hours to disable the contravening information and then preserve it for ninety days for investigation. It has to inform users of its website, or computer resource, that non-compliance of rules and regulations, privacy policy and user agreement shall lead to termination of such access. Further, the intermediary has an obligation to assist government agencies in prevention and detection of cyber security incidents as well as for penalizing offences. Where an intermediary restricts access to information, he shall be liable under, section 69 of the IT Act for maximum imprisonment of 7 years and a fine. Uploading movies, music or TV series on

4 Section 43A provides punishment for breach
5 Section 72A provides punishment for disclosure
6 1 USD = INR 64
7 Rule 2(1)(j) defines a user to mean any person availing services provided by an intermediary to host, publish, share, transact, display or upload information on his website
8 Rule 3(2) details 8 sub-points which an intermediary cannot do and only some of them are listed here

YouTube that violates intellectual property rights, selling illegal products on Amazon, sharing web link containing virus on Facebook, etc. requires intermediaries to disable or remove such content.

Intermediaries have to undertake reasonable security practices and procedures in accordance with the Data Rules, develop and employ means for securing computers and report cyber security incidents to the Indian Computer Emergency Response Team. They must publish on their website, the name and contact details of a grievance officer along with mechanism to be followed by a data giver in case of complaints against access or usage of computer resource of the intermediary. Such officer has to redress complaints within one month from receipt. Where such officer is not appointed, the intermediary shall be liable to pay compensation to the affected person or penalty of maximum INR 25,000 (about USD 400).[9]

Section 79 of the IT Act provides protection to intermediaries if **(a)** they do not initiate and channelize any transaction with available information; **(b)** their functioning involves limited access to communication system containing information of third parties; and **(c)** they conduct proper due diligence. The protection is not available when operations are unlawful and information causing unlawful act(s) is not removed from the platform.

3. The Concerns

3.1 Data Rules

The objective of creating Data Rules was to protect personal and sensitive data belonging to individuals and used by various companies and the government. However, they do not include government organizations within the definition of body corporate. With digitization wave, numerous departments like income-tax, passport, transport offices, etc. collect information of citizen, and lack of proper IT infrastructure and reasonable security practices makes such information susceptible to theft, hack, leak, damage, etc. It is imperative that definition is revised to bring government agencies within the purview of IT Act and Data Rules to protect data and sensitive information. Recently, approximately 200 central and state government websites displayed name and addresses of some Aadhar beneficiaries, thereby, highlighting the weak security measures adopted by government of India to protect data.[10]

Reasonable security practice is determined on a case to case basis, unless ISO standards are followed, in which case, it is deemed. However, even big multinationals find such standards cumbersome and expensive. Thus, feasibility for Indian start-ups adopting ISO appears bleak. In such scenario, extra care has to be taken to ensure that in event of data breach, reasonableness and proportionality of security measures is structured, at all levels with the organization, documented and appropriately caveated and not just kept in the fine print.

Further, information collected by a corporate body should not be held for "*longer than it is required for the purposes for which the information may lawfully be used.*"[11] Using information lawfully would enable a corporate body to retain information for any time period they require on grounds that

9 This penalty is under section 45 of the IT Act
10 https://tech.economictimes.indiatimes.com/news/corporate/210-govt-websites-made-public-aadhaar-details-uidai/61719345, (*Last accessed on December 22, 2017*)
11 Rule 5(4), provides time period for retention of information

information has been retained to improve experience of customers availing there services. Further, after termination of contract between the corporate body and data giver providing consent to use sensitive information, the rules do not provide any method as to disposing of information which exist with the corporate body. It raises concerns as to whether the data shall be deleted, the time period within which it shall be removed and if the data giver shall be informed about such disposal. Therefore, the rules should specify as to what comprises of using information lawfully and inserting a provision for treatment of disposing information held by a corporate body.

3.2 Intermediary Rules

When any post or information posted on Intermediaries website violates Rule 3(2), the intermediary receives a take-down notice from the government authorities for removing such posts or information within thirty-six hours of such upload. The rules require intermediaries to determine whether any content violates the Intermediary Rules and to block, or remove it from its website. It creates issues for the intermediaries dealing with huge data as they do not have the required knowledge and skills to remove information and the information may or may not be unlawful. In the case of *Myspace Inc v Super Cassettes Industries Ltd* [12], Super Cassettes had contested copyright violation of their music uploaded on MySpace, a social platform to share and upload music. MySpace contested that as an intermediary they only provided a platform and had no knowledge of copyright infringement. The Delhi High Court held that intermediaries only serve as a medium to exchange information and are not equipped to pre-screen and verify all information stored on their website. Intermediary would only be liable when he has actual knowledge and not constructive knowledge of infringed content posted on its website which is not removed.

Time limit of thirty-six hours is obscure as intermediaries have different businesses which may require reasonable time to remove any information violating the rules. An intermediary such as Facebook, where millions of posts are uploaded every minute on its website would require more time for removal of any unlawful information than an intermediary as compared to OLX (Indian company providing platform for buying and selling second hand products) which has lesser posts and different operations as compared to Facebook.

An intermediary has to publish the name and contact details of the appointed Grievance Officer on its website, however, it does not provide a mechanism for appointing the officer, addressing grievances, consequences in case of failure to resolve disputes, limitation on his duties, etc.

Intermediary's scope is wide and includes anyone dealing with information and data in any manner. This causes issues and there is an increasing tendency for everyone complying with Intermediary Rules. Therefore, the scope of applicability of Intermediary Rules must be clarified for individuals and corporate bodies handling data and personal information.

4. Conclusion

With increasing digitalization, the Ministry of Information and Technology has put in place the IT Act, Data Rules and Intermediary Rules to secure the information and personal data shared between people and to regulate the work of intermediaries receiving information. However, in practicality, the penalties have been rarely imposed due to which organizations either do not

12 Myspace Inc v Super Cassettes Industries Ltd. & Anr, 236(2017)DLT478

follow the rules or are unclear on the judiciary's stand on data breach. The lack of public information on implementation impacts the core objectives of protecting data and ensuring privacy. It affects the IT/ITES sections credibility in international scenario where western jurisdiction has proactive and stringent implemented measures. The time is ripe to revisit existing law and bring modification to classify and enable better implementation.

Author
Varun Munjal