DATA PROTECTION VIS-A-VIS CORPORATE LIABILITY IN INDIA: MISSING OR INEFFECTIVE FRAMEWORK?

Written by **Atisha Sisodiya* & Ayush Gupta****

* LL.M. Student, Maharashtra National Law University, Mumbai

** LL.M. Student, Maharashtra National Law University, Mumbai

1. Introduction

The 21st century has witnessed, widely referred to as the 'information age', has witnessed a rapid development in digital technology which has posed a huge challenge in regard to privacy and protection of information which is stored in electronic form. The online storage and communication of data has associated risks as much of the information consists of personal details and the computers are now able to process the information that covers all fields of human activities. The digital revolution though holds a great significance in all the sectors of society and has resulted in the Government of India implementing the "Digital India" initiative which involves the incorporation of digitisation in governance; healthcare and educational services; cashless economy and digital transactions; transparency in bureaucracy; fair and quick distribution of welfare schemes etc. to empower citizens.[1] The Internet has brought a revolutionary change and has resulted in an increased visibility of the vulnerability of information and data. As stated by the Supreme Court in Puttaswamy judgement[2]:

> *"'Uber, the world's largest taxi company, owns no vehicles. 'Facebook', the world's most popular media owner, creates no content. 'Alibaba', the most valuable retailer, has no inventory. And 'Airbnb', the world's largest accommodation provider, owns no real estate."*[3]

[1] Press Information Bureau, Digital India – A programme to transform India into digital empowered society and knowledge economy (20 August 2014), available at http://pib.nic.in/newsite/PrintRelease.aspx?relid=108926 (last accessed 16 November 2017).
[2] Justice K.S. Puttaswamy (Retd.) v. Union of India & Ors. 2017 (10) SCALE 1.
[3] Tom Goodwin, _The Battle is for Customer Interface', TechCrunch (3 March 2015), available at: https://techcrunch.com/2015/03/03/in-the-age-of-disintermediation-the-battle-is-all-for-the-customer-interface/

From something as simple as booking an Ola auto or a Uber cab, to using Fitbit to tell if they are walking enough to providing locational data on Google maps, technology has become omnipresent and interactions more seamless. One cannot deny the fact that these applications and technology provide a large number of benefits and are required for various purposes such as, effective planning and implementation schemes of government schemes, delivery of social welfare benefits, counter terrorism operations etc. However, one cannot overlook the fact that such collection and use of data poses certain risks as it collects and analyses personal data from individuals. Thus, both public and private sector are involved in the activity of collecting and using personal data for various purposes. The unregulated use of personal data raised concerns regarding the privacy which was a subject matter of the landmark Supreme Court judgement recognizing right to privacy as a fundamental right.[4] The judgement recognized informational privacy as a facet of the right to privacy and directed the Union Government to put in place a robust data protection regime to ensure protection against the dangers posed to an individual's privacy by state and non-state actors in the information age.[5] In regard to this, to harness the benefits of the advancing digital economy and reduce the harms resulting from it, it was considered necessary to formulate a data protection law for India. For the same, the Government of India constituted a Committee of Experts led by Supreme Court judge, Justice Shri B.N.Srikrishna to study various issues relating to data protection and give necessary suggestions. The Ministry released a white paper on November 28, 2017 which is aimed at securing digital transactions and addressing privacy issues.

This paper seeks to analyse the effectiveness of the present law and the road ahead for the future of legal framework of data protection vis-a-vis corporate liability in India. It analyses the corporate liability issues existing in India and gives suggestion to give complete independence to the corporations with stricter legal regime. In addition to this, the paper analyses data protection in relation to the latest privacy judgement. The paper is structured as follows: Section I is the introductory chapter. Section II analyses the present position of law with respect to data protection and corporate liability in India. The section analyses the White Paper released by the Ministry of Electronics and Information Technology and discusses two

(last accessed 14 November 2017) cited in Justice K.S. Puttaswamy (Retd.) v. Union of India & Ors. 2017 (10) SCALE 1, Per S.K. Kaul, J. at paragraph 17.

[4] 2017 (10) SCALE 1.

[5] 2017 (10) SCALE 1.

issues which from the heart of the debate. Section III throws light on some corporate liability issues in India. Section IV draws reference to the practices of various international jurisdictions such as the European Union and the United States. Section V is Suggestions and Conclusion.

2. Present Position of Law With Respect to Data Protection and Corporate Liability in India

The data protection issue is back in the limelight with the publication of a 243 page white paper by the 'Committee of Experts' led by former Supreme Court Judge, Justice B.N. Srikrishna. The Ministry of Electronics and Information Technology released the white paper aims at securing digital transactions and addressing privacy issues and gives a deep analysis on some core issues and welcomes comments from public. It seeks response to 231 questions covering a broad spectrum of issues relating to data protection – including definitions of terms such as personal data, sensitive personal data, processing, data controller and processor – the purposes for which exemptions should be available, cross border flow of data, data localisation and the right to be forgotten.[6]

There are two issues that form the heart of the debate. The primary question that needs to be answered is whether India needs one data protection law to include both the public and private sector. Another issue that stems from the first is that whether the state should be bestowed with complete authority to create a data protection authority that will act as a regulator for both private and public sectors.

2.1 One common law for the public and private sector or different laws for both?

The white paper touches on this issue but does not adequately provide information regarding the pros and cons of both. In the opinion of the researcher, there is a need to analyse this issue in regard to the latest Puttaswamy judgement[7]. The judgement is not clear in regard to the horizontal applicability of the privacy right vis-à-vis private citizens. Justice S.A. Bobde seems to be of the opinion that the fundamental right would be applicable only against the state and that the private citizens could only claim a common law right to privacy against each other.

[6] https://thewire.in/201123/inclusive-co-regulatory-approach-possible-building-indias-data-protection-regime/
[7] Justice K.S. Puttaswamy (Retd.) v. Union of India & Ors. 2017 (10) SCALE 1.

However, Justice S.K. Kaul states that privacy as a fundamental right could apply even against private citizens.

If privacy as a fundamental right is to be recognized vis-à-vis the state only, then there is no logic to cover both public and private sectors under the same data protection law because the underlying legal basis of both the sectors is entirely different. The nature of the Indian citizens' relationship with the Indian state is almost always coercive and the information that the state extracts from the citizen pursuant to an exercise of its coercive powers should be placed at a far higher standard of privacy protection when compared to information that the citizen-consumer voluntarily hands over to a private company in pursuance of a contractual relationship.[8]

If the issue of data protection for both public and private sectors is brought under the same law then there may be jurisdictional conflicts between the information commissions and data protection regulators. The law will have to draw a line between transparency under the Right to Information Act, 2005 and privacy under the prospective data protection law, with regard to public records. This may give rise to concerns regarding what information can come under the ambit of 'informational privacy' and how much information should go behind the veil of privacy.

2.2 One data protection authority for all?

The second issue that stems from the first is the creation of a data protection authority as a regulator that will have powers to punish both public and private sectors across the country for any violation of privacy or data protection laws. As per the white paper, it appears that there is going to be one big regulator that will have punitive powers. This may result in serious consequences as so much power will be given in the hands of one single authority that will not only have the power to inspect records and data but also levy fines which might bankrupt businesses and regulate Indian companies with enough red tape to make them uncompetitive in a global marketplace.[9]

[8] https://thewire.in/202497/data-protection-law-regulator-india/
[9] Prashant Reddy, *Does India Need Only One Data protection Law and Regulator to Rule Them All?* 7 Dec, 2017 available at: https://thewire.in/202497/data-protection-law-regulator-india/

At present, the government has less control in regard to regulating and controlling social media platforms like Facebook, Twitter and Google but if the entire regulation is handed over to one data regulator, it may result in accumulation of powers in one hand. It has been said that the European model of data protection is being fused into the Indian system because it has great resonance within the Indian bureaucracies and activists. The Indian democracy but one has to understand the fact that the functioning of Indian bureaucracy and the political system is very different from that of Europe. The European model puts a lot of restrictions on processing data and has a central bureaucracy that enforces such a framework. Thus, it has a complex data regulatory framework. Our system of governance is too centralized. Creation of one centralized powerful data protection authority will contribute even more to the centralization of power and will have ramifications for liberty, freedom and economic competition in 21st century India. Replicating an out-dated model of European data regulation, which even the Europeans are struggling to implement or integrating the European method of regulation with a coercive Indian political may prove to be a disaster.

3. Corporate Liability issues in India

In India, there is no comprehensive data protection law like EU, so the data protection issues at present are addressed by the Information Technology Act (IT Act) and Rules. Section 43 of the IT Act does not provide any clarification regarding the liability of corporate bodies. The term "reasonable security practices" though has been defined, it does not provide for a detailed clear procedure that needs to be followed. Further, there is no specification of upper limits for the compensation. The rules require the body corporate to publish privacy and disclosure policies for personal information however this is has a very wide coverage. Such an obligation is not considered desirable as the corporate bodies have all kinds of information and there is no clarity provided regarding what kind of data is to be protected. The White paper can be expected to provide a new comprehensive regime for data protection. It contains provisions of appointment of data controller by the appropriate government and the corporate bodies will be required to report to the Data Controller about the type of personal information and data collected by them and the purpose for the same. However, the white paper does not mention anything about self-regulation by the corporate bodies. They are required to report to the data controller and take adequate, measures for confidentiality and security however there should be provisions whereby the corporations can also get a chance to establish a procedures and

legal obligations themselves in a contractual framework which may be subject to the approval of the data controller.

The absence of a comprehensive data protection law in India can be considered to be a loss to the outsourcing industry as, though it is a flourishing industry; it does not have a proper framework for data protection. In US and EU, the customers have complete protection under the privacy directives which states that their personal data cannot be transferred to countries which do not have an adequate data protection policy. As a result of this, data protection is taken consideration in international outsourcing companies. In India, this may lead to a block in the outsourcing industry which may be hampered by the bar on transfer of information because it does not have the same level of data protection measures. Such a bar would mean that the outsourcing companies cannot send data to their employers, employees or other offices located in different jurisdictions which do not have the same level of data protection and the same may lead to loss of business opportunities.[10]

4. International Practices

To analyse India's approach to data protection, understanding the practices followed in other jurisdictions like United State and European Union is necessary. There are two distinct models in the field of data protection: The European Union (EU) model and the other similar models suggest for a comprehensive data protection law and the American model suggests for a sector specific data protection law system. This is because of the distinct conceptual basis for privacy in each jurisdiction[11]. The two approaches are briefly discussed below:

4.1 European Union

In EU, the European Charter of Fundamental Rights (EU Charter) recognises the right to privacy in Article 7 as well as the right to protection of personal data in Article 8. The first principal EU legal instrument on data protection was the Data Protection Directive.[12] The

[10] Anuradha Parihar & Aratrika Chakraborty, *Data Protection and Corporate Liability: Balancing of Law and Self-Regulation*, International Journal of Law and Legal Jurisprudence Studies, Vol.3 Issue 2

[11] Avner Levin and Mary Jo Nicholson, *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, 2(2) University of Ottawa Law & Technology Journal, 357 (2005).

[12] The European Union Agency for Fundamental Rights (FRA), the Council of Europe and the Registry of the European Court of Human Rights, Handbook on European Data Protection Law (2014), available at: http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf, (last accessed 4 November 2017).

Directive was adopted in 1995 and is based on the OECD principles.[13] UK has enacted the data protection act 1998 based on this directive which replaced the 1984 Act. The directive has made the scope of security aspects and corporate liability clear but there are still several issues relating to it.

The new framework that has been proposed seeks to provide for a stricter legal regime for data protection. Personal data can only be collected legally under strict conditions and for a legitimate purpose. In addition to this, the organisations or persons who collect and gather such information have the duty not to misuse it and are expected to respect certain rights of the data owners. The changes suggested in the new framework will place a burden on the corporations. Firstly, since it's a regulation and not a directive, it will be binding on all the member states. Secondly, the corporation has to keep a data protection officer dedicated for the purpose of data protection rules and procedures and have to be more clear on the aspects and reasons of data transfer and data processing.[14]

The kind of data protection regime which is being proposed will have to be assessed from the point of view of corporations because when the legal approach is more and more changing to a self-regulated and contractual provisions framework with the invalidity of the safe harbour provision whether such kind of stricter laws would be desirable has to be seen.

4.2 United States

In United States, there is no single comprehensive law which regulates the collection and use of personal data. Instead, there is a patchwork of federal and state laws and regulations which sometimes overlap and contradict each other. In addition to this, there are various guidelines which have been developed by governmental agencies and various industry groups that do not have legal powers but are part of self-regulatory guidelines and frameworks that are considered

[13] The Organization for Economic Co-Operation and Development, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,<http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.
htm> accessed 25 October 2015

[14] See, Dan Worth, *EU data protection law overhaul: everything you need to know*, < http://www.v3.co.uk/v3-uk/news/2413351/eu-data-protection-law-overhaul-everything-you-need-to-know> (last accessed 26 February 2018).

to be "best practices". Some laws apply to a specific category of information, such as electronic communications, financial or health information. Some of the major federal laws include:

a. Federal Trade Commission Act: This Act is a federal a consumer protection law that prohibits unfair or deceptive practices and applies to most companies and individuals who are engaged in business, other than financial companies, transportation and telecommunications because these companies are regulated by other national agencies.
b. The Gramm-Leach-Bliley Act: This Act is also known as the Financial Services Modernization Act and regulates the collection, use and disclosure of financial information. It applies to financial institutions like banks, insurance companies, securities firms etc.
c. The Health Insurance Portability and Accountability Act (HIPPA): This Act regulated medical information and applies to health care providers, pharmacies and other organisations that have medical information.

Others apply to activities such as telemarketing and commercial e-mail which use personal information. Further, there are consumer protection laws that are not privacy laws per se but have been used to prohibit unfair or deceptive practices involving the disclosure of, and security procedures for protecting, personal information.[15] There are certain laws at the state level that regulate the collection of personal data. Most states have enacted some form of privacy legislation but however California has multiple privacy laws and leads the way in the privacy arena. For example, the California Security Breach Notification Law applies to persons or business that conducts business in California and owns computerised data that includes personal information, The California Online Privacy Protection Act applies to an operator of a commercial website, online service or mobile app, that collects personally identifiable information through the internet about individual consumers residing in California who use or visit its commercial website or online service.

5. Suggestions and Conclusion

The various legal frameworks for data protection suggest that there is a growing pressure on corporations on data protection liability. It can be seen from the upcoming laws being proposed in various countries, be it EU, US or India, that the laws will pose all the more stricter liabilities,

[15]https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1

both in terms of criminal and compensatory provisions. The present framework in India is ineffective as there is a need for corporations to be given a space for implementing their own regulations with respect to data protection so that they can manage the free flow of the huge amount of information which they need to handle or else it might result in negative implications which may affect the business operations. The corporations must be given complete independence with stricter legal regime. This can be ensured when there is a balance of law and regulation which can be seen when a regulating body oversees the self-regulatory provisions and permit them accordingly. It is time that we must move our country past its existing consultative processes for rule-making as it often results in stakeholders taking adversarial and one-sided positions.