DATA PROTECTION AND CORPORATE LIABILITY: BALANCING OF LAW AND SELF REGULATION

Anuradha Parihar and Aratrika Chakraborty[1]

Abstract

The advent of digital age has posed an increasing challenge for the privacy and protection of electronic data. The corporate liability which rests on the corporations for protection of personal data which they handle is an increasing concern for the free flow of information in international commerce. Several upcoming laws which are being proposed whether in EU, US and India propose to pose all the more stricter liabilities whether in terms of criminal or compensatory provisions. However, the need of the hour is the balance of self regulations and legislations. There are several factors to be considered whenever we are trying to establish a framework of corporate liability for data protection. Most of the big corporations have a trans-national character of work in this global age and establishing a rigid and one way approach to data protection regime can be detrimental to the future of a healthy economy. The corporations have to be given a space for implementing their own regulations with respect to data protection to manage the free flow of the huge amount of information which they need to handle. Otherwise the implications are going to be negative in terms of efficient business performance. 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. The whole country at this juncture is seeking to have an all comprehensive legislation for data protection as EU is having, however it is also necessary to understand and determine the ambit and scope of its applicability so that the liability regime is justified and certain in ensuring the optimum and desired results.

Keywords : electronic data, corporate liability, personal data , self regulation.

INTRODUCTION

With the advent of digital age, there has been a revolutionary change in the concept of data storage and processing. Most of the information is now being stored in an electronic form. Whenever there is an online storage and communication of data then there are associated risks by hackers and perpetrators of accessing those information to the detriment of the provider or the legitimate user.

Corporations who are regularly in the process of storing and dealing with personal and sensitive data of their clients and, employees are very much vulnerable to these kinds of perpetration, which can take place from either some outside hacker or even subjected to some internal sabotage. So it becomes very necessary to apply some kind of security mechanisms to ensure the safe storage and usage of these data. There can be legislations to ensure the corporate liability or

[1] Anuradha Parihar, LLM (Cyber Law & Cyber Security), NLU Jodhpur and Aratrika Chakraborty, LLM (Cyber Law & Cyber Security), NLU Jodhpur

even the corporations can deal with it with the mechanisms of appropriate self regulations within the institution.

However, there also exists the other side to the coin of this regulatory mechanism. The corporations are the backbone of the economy of a particular state or even globally. There are several factors to be considered whenever we are trying to establish a framework of corporate liability for data protection. Most of the big corporations have a trans-national character of work in this global age and establishing a rigid and one way approach to data protection regime can be detrimental to the future of a healthy economy. There can be vague or convoluted legislative provisions which prove to be insufficient to establish a proper corporate liability regime. Or there can be a hindrance to the free flow of information in a international sphere in certain instances where it is necessary and desirable. Even in certain situations the claims which arise in cases of security breaches in data protection may be unwarranted in those situations and may pose an undesirable situation for the business of the corporation.

The nature of the transaction which the corporation is carrying out is also a determining factor to be considered while analysing and determining their liability, Also the nature of the data which is being stored and processed is a key factor. The ambit of Sensitive personal data or information ("SPDI") is very necessary to understand and how far and to what extent it is justified to put the burden of protection on corporations.

India presently does not have any data protection legislation per se but it has provisions of corporate liability in IT act and the rules. However a data protection bill[2] which is being proposed in the parliament for a long time since 2006 , is being awaited. 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. The whole country at this juncture is seeking to have an all comprehensive legislation for data protection as EU is having, however it is also necessary to understand and determine the ambit and scope of its applicability so that the liability regime is justified and certain in ensuring the optimum and desired results.

PRESENT POSITION OF LAW IN WITH RESPECT TO DATA PROTECTION AND CORPORATE LIABILITY IN INDIA

The concepts of privacy were introduced in the Information Technology Act,2008 by way of section 43A (Compensation for failure to protect data) and 72A (Punishment for disclosure of information in breach of lawful contract) in order to deal with the problems of data privacy and data protection.

Section 43A specifically deals with body corporate and provides for compensation if any body corporate dealing with sensitive personal data and information is negligent in implementing and maintaining reasonable security measures for the same. The provision provides for an upper limit with regard to the compensation and also an explanation for the terms like 'body

[2] The Personal Data protection Bill, 2014

corporate', 'reasonable security practices and procedures' and 'sensitive personal data or information'.

Section 72A deals with a situation where personal information is disclosed in breach of a lawful contract or without the consent of the information provider. This section provides for punishment if a person or an intermediary having access to personal information of a person under the terms of lawful contract discloses the same in breach of such lawful contract or without the consent of the information provider.

The Ministry of Communications and Information Technology, Government of India on 13 April 2011, notified the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 also known as the IT Rules. These Rules set out the reasonable security practices and procedures that must be followed to protect the sensitive personal data. The rules were framed to bring in certain clarification like the definitions of sensitive personal information, body corporate, the reasonable security practices and procedures etc.

Rule 2(1)(c) in order to define "Body Corporate" refers back to the meaning of body corporate given in the explanation to section 43A of the Information Technology Act. Thus the term 'body corporate' is understood to mean *any company and includes a firm, sole proprietorship or any association of persons engaged in a commercial or professional activities.*

Rule 3 defines the "Sensitive personal data" (SPDI) which was not defined by the IT Act instead found mention in the explanation of section 43A only to mean any personal information prescribed by the Central government. So, the Rules give an inclusive definition of the same under which a list of information is covered like passwords, financial information, information relating to physical, physiological and mental health condition, sexual orientation, medical records and history, biometric information of an individual along with any such information provided to body corporate for providing of service and also any such information received by the body corporate under a lawful contract. This rule also provides that any information which already exists in the public domain would not amount to sensitive personal data or information for the purposes of these rules. Thus SPDI has been clearly elaborated in the rules and liability has been established for any breaches with respect to it.

The body corporate or any person who on behalf the body corporate collects, stores, receives, processed or handles personal data is obligated to prescribe privacy policy for handling such personal data and publish the same.[3] The usage and collection of any kind of information or SPDI can be done only with the prior consent of the data provider and for a lawful and necessary purpose only.[4]

[3]Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 4

[4] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 5

Even all the disclosures to the third party has to be done with the prior permission from the provider of such information provided under the legal contract unless either its agreed in the contact or its for fulfilment of a legal obligation.[5].

Rule 7 provides that the sensitive personal data can be transferred by the body corporate to any other body corporate or person in or outside India if the said body corporate maintains the same level of data protection adhered by it. But such transfer is allowed only in case its necessary for fulfilment of lawful contract.

Rule 8 in a way elaborating the law under section 43A of the IT Act clarifies that reasonable security practices and procedures has to be followed by each body corporate and the International Standard shall be followed.

The liability on corporations who have been outsourced the processing of some personal data becomes a problematic area therefore to clarify the position with respect to outsourcing companies the Department of Information Technology of the Ministry of Communications and Information Technology issued a press note on 24 August 2011 that was published on the website of the Press Information Bureau. As per this an independent BPO industry providing the services of collection, storing, dealing and handling of sensitive personal information under a legal contract with a legal entity or a company shall not be liable to obtain consent from information provider for collecting or for disclosing the same no matter whether the information provider is in or outside India. However any back office of the company in direct contract with the information provider shall be liable to obtain such consent in writing from the information provider even if he is outside India. Thus, the outsourcing companies in India are exempted from the provisions of collection and disclosure as set out in the IT Rules.[6]

DATA PROTECTION REGIME: AN INCREASING DISRUPTION IN FLOW OF INTERNATIONAL COMMERCE

In the digital age, with the increase in the amount of data being stored the risk of becoming targets of cyber-hacking is also increasing. The businesses which store its client information including bank details and other personal details of them can become targets of such cyber-hackers. There exists an immense amount of responsibility on part of corporate bodies to protect such information collected and maintained by them. Though majority of the security breaches are done by outsiders but the cases of such breach by insiders have also been in rise.

Laws in certain countries obligate the companies to notify the affected individuals about such kind of breach of their personal information which might still lead to a class action against them

[5] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 6

[6] *Clarification on Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 Under Section 43A of the Information Technology ACT, 2000,* Ministry of Communications & Information Technology (Dept. of Information Technology), Press Information Bureau, August 24, 2011

alleging that the company was negligent in securing the confidential information. Such class actions expose the companies to bad publicity and also economic losses. Though, nearly all of the class action suits that have been brought against companies in the wake of data breaches have failed[7] however, the economic loss doctrine applies as it can be seen that most of damages suffered by the plaintiffs in such cases are speculative viz. it cannot be quantified as the information stolen does not have any pecuniary value. Thus, problem of computation of the amount of damage comes in.

Law enforcement Compliances

The government poses constant pressure for compliance with the law enforcement and other regulatory requests on the companies which deal with processing of data in multiple countries wherein these requests consists of access to such personal data by the government. However, the problem arises because such compliances if made are in conflict with data protection and privacy laws of those countries where these companies operate. *The data protection and privacy laws of the countries where the individuals are located may also "attach" to their personal data and continue to apply as these data are transferred internationally, so that such laws may be violated if the data are subsequently disclosed to foreign law enforcement authorities*[8].

At times the disclosure of personal data on the request of authorities lead to violation of the commitment the companies make towards its customers and employees. Moreover such a violation may to lead to loss of reputation for the company. The flow of international commerce may also be disrupted because of the negative impact created on the companies' decision due to the legal and political risk involved in such conflict of laws. Political tensions between countries may arise when law enforcement authorities in one country request companies to disclose personal data collected or stored in another one, and companies may be caught in the middle.[9]

Corporate Liability Issues in the EU and US Regime

To analyze the legal and economic connotations for the corporations with respect to the existing and upcoming Data Protection legal framework in our country understanding the impact of the existing data protection laws in other jurisdictions like EU and US becomes very necessary.

European Union

The Data Protection Bill pending in our Parliament is expected to be on similar lines of EU Data Protection Directive (Directive 95/46/EC). In EU the European directive on data protection adopted in 1995 is based on the OECD principles[10]. UK has enacted the data protection act 1998 based on this directive which replaced the 1984 act.

---

[7] Jeremy Chang, 'Data Breach and Corporate Liability'(2013) CBLR <http://cblr.columbia.edu/archives/12873> accessed 25 October 15

[8] ICC Commission on Digital Economy, *Cross border law access- Current issues into under data protection and privacy law,* 2012

[9] *Ibid*

[10] 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

Though this directive has made the ambit of security aspects and corporate liability clear there are several issues connected to it.

Many problems are posed in cloud computing services. Cloud computing provides flexible, location-independent access to computing resources that are quickly and seamlessly allocated or released in relation to demand; the services are abstracted and typically virtualised, generally being allocated from a pool shared as a fungible resource with other customers[11] which are trans-border in nature per se. Under the DPD there cannot be transfer of data to a country if it does not follow the European directive standards.

Under the Safe Harbor Agreement which was a framework negotiated by the European Union and the American Chamber of Commerce, there can be transfer of data if the US companies essentially self asses and decide that their level of protection is "equal" to that of EU standards. However in October 2015[12], this principle was held invalid, so unless there is are placement of the agreement by EU and US it can be assumed that mainly contractual clauses or self regulations by the corporate will be used when data is being transferred from EU to US. This approach can serve as a better alternative because the corporations can choose their contractual clauses with consensus and thus an optimum level of protection can be ensured. Here the corporations are getting the maximum liberty and decisiveness to decide on their level of data protection and rules therein. In cases where the corporations feel that the trans border exchange of information will act as a bar to their standards of data protection then provisions to that extent ensuring restrictions can be incorporated in the contracts instead of having a full bar on the transfer of data.

Recently there have been some leaked reports by the presidency which reveal that the EU governments are in disagreement over the issue that whether a consumer should be allowed to go for just compensation in case of that breaches or can sue the corporations. In most cases the entire liability rests on the data controller and the data processor who may be actually responsible for the data breach may not be liable so some EU governments feel that if the data controller and the data processor are both responsible for the data breach then the liability should also be shared and therefore sue each of the businesses i.e. one who is the data controller and another who is the data processor. However problem could arise if the data processor is suppose an entity outside the jurisdiction of the country of the claimant therefore it would be a better alternative to just claim damages from the data controller instead of going for suing the corporations. But such kind of approach would be unfair because the entire burden is on one entity to pay the damages who may not be responsible actually for the data breach. So fixing a liability in these cases is a major issue and becomes a problematic area.[13]

The member states have agreed for a major overhaul to the data protection regime which would be more tough and have a pan-European approach instead of being confined to just within

[11] Millard Christopher,Walden Jan,Hon W. Kuan/Cuningham Alan, Response to the UK Ministry of Justice's Call for Evidence on the European Commission's Data Protection Proposals (March 5, 2012) Queen Mary, University of London, 1, < http://www.cloudlegal.ccls.qmul.ac.uk./docs/65220.pdf > accessed 24 October 2015

[12] See Cara Mcgoogan, 'Safe Harbour deal ruled invalid by top European Court' <http://www.wired.co.uk/news/archive/2015-10/06/safe-harbour-invalid-european-court-justice> accessed 24 October 2015

[13] See, 'EU Governments in disagreement over data breach liability rules',< http://www.out-law.com/en/articles/2015/june/eu-governments-in-disagreement-over-data-breach-liability-rules/> accessed 24 October 2015

Europe. The new regulation seeks to ensure a more strict framework for data protection. The major changes which are proposed will place a huge burden on the corporations from an economic point of view as well as from operational point of view. First of all this is a regulation and not a directive, which means that it will be binding on all the member states. The new law will impose heavy fines which may extend to a 2 percent of a firm's global turnover. Also according to the new law the corporations can be held liable irrespective of their home locations if they are operating in Europe. Also 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]

All these provisions can detrimentally affect the firms operations and so it has been suggested that the there should be a kind of grace period given to the firms for the implementation of the new law. 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.

United States of America

In US there is no single national law which regulates the area of data protection. There are several federal and state laws and also regulations by government and industry groups which comprise the entire gamut of data protection law. Some of such major federal laws include The Financial Services Modernization Act (Gramm-Leach-Bliley Act (GLB)) (15 U.S.C. §§6801-6827) that regulates the collection, use and disclosure of financial information of financial institutions such as banks, securities firms and insurance companies, and to other businesses that provide financial services and products and The Health Insurance Portability and Accountability Act (HIPAA) (42 U.S.C. §1301 et seq.) that regulates medical information in the possession of health care providers, data processors, pharmacies and such other entities

The recent act in US which is being proposed by the Congress is sought to create a national data protection and breach notification law that, in theory, would increase the security of consumers' personal information and simplify the data breach notification process. There is an increased accountability and requirements for corporation to comply with security practices and there are also strict compensatory provisions. The act applies to government agencies and interstate businesses with the exemption of financial institutions subject to the Gramm-Leach-Billey Act and businesses bound by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Services providers that act as intermediary agents in transmitting, routing and data storage are also exempted.[15]

The bill is clearly designed to prevent businesses from mining information from consumers. It's clear that if a company doesn't take the proper precautions to encrypt or obscure customer information, that the federal government is going to be intent on pursuing restitution from the

[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> accessed 26 October 2015

[15] Jared Magill, 'The Crooked Path to Determining Liability in Data Breach Cases', <http://www.wired.com/insights/2015/03/crooked-path-determining-liability-data-breach-cases/> accessed 26 October 2015

company. The measure enacted by Congress puts limits on the type of information that a company can collect in the first place. Additionally, strict timelines require that companies must purge information after a certain amount of time. This could put companies that engage in quasi-financial operations, such as companies that act solely as merchant processors, at risk of losing valuable information on specific individuals.[16]

The proposed act will serve as a major wake up call to the corporations on stricter liability regime for data protection and a huge burden of IT infrastructure would be now necessary. The compensatory provision approach may not fully desirable as discussed previously because these kind of claims in civil actions where personal injuries are involved are precisely immeasurable and an impractical liability on the corporation in many cases. There should be a kind of mechanism whereby the corporations may themselves be able to self regulate the retention time of the data according to its nature and usage and a blanket limitation on the data retention time period should not be there.

Corporate Liability issues in India

The data protection law in India is partially addressed by the act and rules but it is not a comprehensive data protection law like EU. As per S. 43A of the IT Act the liability on corporate bodies also seems to be a bit shaky because "reasonable security practices" though have been defined but there cannot be an exhaustive and clear procedure which needs to be followed, and so this is not clarified properly. Moreover there are no upper limits specified for the compensation. Data breaches relating to SPDI cannot be objectively compensated in terms of exact amount so this is a problematic area.

The rules require the body corporate to publish privacy and disclosure policies for personal information however this is has a very wide coverage.[17] Such sweeping obligation on corporate bodies which handle all kinds of information is not desirable because it should be made clear as to what kind of data exactly the statute is seeking to protect. All kinds of personal data is not practically possible to provide equal protection for.

The absence of Data Protection Law in India is a heavy loss to the outsourcing industry as though it is a flourishing industry in India but does not have a proper Data Protection Act. The customers in the US and European Union are protected by the comprehensive privacy directive which requires that the personal data cannot be transferred to countries which do not have adequate protection policy. As a result the European trade Union finds that data protection is a major issue which has to be taken into consideration in these international out-sourcing companies. Hence this may lead to a block in the out-sourcing industry in India.[18]

The bar on transfer of information to other countries which do not have the same level of data protection measures may also hamper the outsourcing industry in India. Such bar would mean

[16] *Ibid*

[17] See, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 4

[18] Danish Jamil, Muhammad Numan Ali Khan, 'Data Protection Act in India with Compared To the European Union Countries' (2011) Vol: 11 No: 6 IJECS-IJENS <

that the outsourcing companies cannot sent the 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.

The Personal Data Protection bill which is presently pending in the Parliament can be expected to provide a new comprehensive regime for data protection. The bill makes provision of appointment of a data controller by the appropriate government and the corporate bodies will be required to report to the Data Controller the type of personal data and information being collected by them and the purpose for which it is being or proposed to be used.

The bill does not talk about any provision of 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. Taking away the self regulating aspect altogether is not desirable.

Moreover the bill has widened the ambit of the privacy breach by including personal data instead of segregating between SPDI and personal data. The level of obligation is same for all kinds of personal data. If we see the UK Data Protection Act, 1998 there are different levels of requirement for personal data and sensitive personal data. SPDI has been separately classified and therefore Where the information concerned is sensitive personal data, at least one other of the Schedule 3 conditions set out in the DPA must also be met before the processing can comply with the First Data Protection Principle that personal data must be processed fairly and lawfully. The processing of sensitive personal data will usually require the individual's "explicit consent" (see Schedule 3 DPA).[19]

As discussed previously also as a corporate body the information it needs to process is huge and it is not practically possible to impose the same level of obligations for all kinds of personal data. Personal data has been defined as

(c) "personal data" means information or data which relate to a living individual who can be identified from that information or data whether collected by any Government or any private organization or agency;

So it can be seen that the ambit is very wide and there needs to be proper clarity on the aspect of liability dealing with SPDI and personal data as such.

CONCLUSION

As can be seen from the various legal frameworks for data protection there seems to be more and more increasing pressure on corporations on data protection liability. Several upcoming laws which are being proposed whether in EU, US and India propose to pose all the more stricter liabilities whether in terms of criminal or compensatory provisions. However, the need of the

[19] Data Protection Act, Administrative Data Liasion Service, <http://www.adls.ac.uk/adls-resources/guidance/legal-guidance/data-protection-act/> accessed 26 October 2015

hour is the balance of self regulations and legislations. The corporations have to be given a space for implementing their own regulations with respect to data protection to manage the free flow of the huge amount of information which they need to handle. Otherwise the implications are going to be negative in terms of efficient business performance. One of the ways to ensure the balance of law and self regulation is that a regulating body may oversee the self regulatory provisions and accordingly permit them. But an overall independence to the corporations is a must with the stricter legal regime.