IOSR Journal Of Humanities And Social Science (IOSR-JHSS)
Volume 20, Issue 8, Ver. II (Aug. 2015), PP 34-43
e-ISSN: 2279-0837, p-ISSN: 2279-0845.
www.iosrjournals.org

Personal Data Protection Laws Concerning Bangladesh

Himaloya Saha[1], Saquib Rahman[2]
[1]*Postgraduate (LL.M.) student, University of Warwick, UK*
[2]*Postgraduate (LL.M.) student, University of Warwick, UK*

Abstract: *This paper contains the concept of Personal Data, the effect of data being misused and the suffering of the individuals due to such misuse in many cases. It focuses on the need for personal data protection laws to be enacted in Bangladesh. Reflections have also been made on the laws prevailing in Bangladesh (such as the Contract Act 1872 and the Information and Communication Technology Act 2006) in respect of personal data privacy and how inefficient they actually are compared to the reality prevailing in the country. For strengthening such a law, eight basic principles have been mentioned for implementation of the rights that are possible to be guaranteed. Then the paper goes on to elaborate about personal data protection laws falling within the range of right to privacy in the context of the Constitution of The People's Republic of Bangladesh. Recommendation as to how an Act may be made, protecting personal data of individuals has been highlighted. In conclusion, emphasis has been made for the immediate requirement of a Personal Data Protection Law to ensure proper security of data. Penalties and remedies thereto for non-compliance of the law have been put forward for consideration, as prevalent in many developed countries of the world.*

Keywords – *Personal Data, Data Protection, Personal Data Protection Act, Intellectual Property Bangladesh*

I. Introduction

In today's globalized world, technological advancements have reached to an extent that people are required to generate personal data more often than not. Personal information apart, it is also used for fighting terrorism in the modern world. It is a matter of concern how personal data is being used within the paradigm of freedom, security and justice.[1] Considering the expansion of e-commerce, cloud computing, social networks and online games, a law is required to be formulated concerning protection of personal data needed to be modern enough to provide with security online.[2] World where dependence on technology is to a great extent today, Personal Data Protection laws are being enacted in many nations. Enforcements, implications, limitations and the need for incorporating Personal Data Protection laws are mentioned and well discussed in various legislations and articles of different countries. However in this research, unfortunately we did not come across any such quality write-ups/articles worth mentioning, that states regarding personal data protection laws in Bangladesh.

I.I Historical Background

Going into the history with regards to Data Protection, enacted in the form of a Data Protection Act in the year 1970 in the German State of Hesse was the first ever computer specific statute. People were concerned regarding the misuse of records under the regime of the Nazi, with regard to usage of computers in order to store and process large amounts of personal data. The Data Protection Act was thus pursued to resolve the concerned problems.[3] In the year 1973, an introduction of data protection legislation was seen in the case of Sweden and that was the first national statute.[4] In 1981 the Council of European Convention established standards among member countries, to ensure free flow of information among them without infringing the personal privacy. Three years later the first Data Protection Act was introduced in UK. It made it mandatory for public and private organizations about access to computer-held personal data for registering with a Data Protection Registrar. However it is to be noted that it did not explicitly recognize the individual's right to privacy. That changed the Data Protection Act 1998, which was built on an EC directive of 1995 and was introduced with the explicit aim of protecting the right to privacy. It specified conditions for the processing of data, tightened restrictions on the use of particularly sensitive information and broadened the definition of data. Moreover, it also separated the functions of registration and enforcement and increased the powers of what is now known as the Information Commissioner.[5] Thus in Bangladesh as well, there is immediate need of a law that would guarantee rights to the people giving out their personal information and make the people accountable for controlling and processing such misdeeds or misuse.

An article the title of which is 'Data Protection and the Information Technology Act in India' mainly mentions regarding Data Protection in terms of The Information Technology Act and other related legislations in India[6], whereas this paper talks about Personal Data Protection in view of the Information and Communication Technology Act in Bangladesh. On the other hand, author of 'Promises and Illusions of Data Protection in Indian Laws'[7] has spoken of the constitutional basis of Data Protection laws which seems similar to this paper, but then again how this paper is different from the mentioned is that the author there emphasized more on how the law is a requirement taking the economic scenario of the country into consideration whereas the following paper states the necessity of the concerned law regarding the legal perspective.

II. Understanding What Personal Data Protection Is

For the purpose of knowing regarding personal data protection, it is immensely important to understand what personal data is and under what circumstances personal data is given out by the people. Personal data means the data that basically relate to a living individual who is identifiable from those data or from those data and other information which are in the possession of, or is likely to come into the possession of the data holder, and comprises of any expression or opinion with regards to the individual.[8] Furthermore, there is something called the Sensitive Personal Data as well. All these require special protection. The information in this includes the ethnic or racial origin, opinion which is regarded to be political, religious beliefs or of similar nature, sexual life, commission or alleged commission of any offence or proceedings relating to offences. The list extends to an extent that people even believe financial documents or their age being mentioned to be 'sensitive'.[9] Why it is probably distinguished is that such information may be used in a manner where one may be discriminated or feel violated about the disclosure of such data.

Common personal information that is collected may be one's name, address, telephone/cell numbers, date of birth, gender, credit-card information, photocopies of identification cards or passport and so on. The protection of personal data goes to an extent that an individual may be identified as long as that person is capable of being identified in the sense of being differentiated from any other individual. For instance, an email address which may clearly identify someone or maybe a CCTV footage that brought out an image that can be matched with a particular photograph, physical description or a physical person.[10]

Practice of giving out personal data is usually to legal entities such as companies or government/public authorities, hospitals or educational institutions. Considering personal data provided to a legal entity such as a company or bank, or even any other service or product providing company requires the personal information for the purpose of processing consumers' orders and managing and administering their account; delivering any services, products or information requested by them, responding to complaints or account enquiries, administering debt recoveries, verifying ones identity when required.[11] Educational institutions require information for the purpose of academic performance of the students (grading sheets and feed backs), access to certain facilities such as the computer labs or library, administration purposes etc. The educational institutions, therefore, often give access to the students of what information they have provided and to be able to check the validity of such.[12]

Hence it can be deduced from the above that the misuse of the personal data and destruction or alteration of that has to be prevented and, therefore, the use of personal data protection laws are necessary.

III. Reasons For The Requirement Of Personal Data Protection Laws

To start with, Personal data protection relates to processing of data which basically means obtaining, recording or holding the data and operating on those via organization, adaption, alteration, retrieval, consultation or use or disclosing it by transmission or in any other manner making it available and also consider the alignment, combination, blockage and erasure or destruction of the data.[13] Provided the information is Sensitive personal data, a person providing the data is required to give his/her explicit consent to the processing of personal data, or data required by law for employment purposes, the data required for the purpose of protecting the vital interests of the individual or other person or data required to deal with the administration of justice or legal proceedings.[14] In light of the above, taking into account personal data being processed in Bangladesh at present, the country has The Right to Information Act 2009 that states provisions in order to ensure free flow of information and people's right to information. The mentioned Act states that any information which may offend the privacy of one's life, any information which may endanger one's life or physical safety of any person, any information given secretly to assist the law enforcing agencies, or any personal information protected by any law, are not subject to mandatory disclosure by government and certain private organization.[15] Violation of the provision is not impossible, and therefore, it is vital that the data are protected via taking legal action.

In respect of the fact that the world is moving so fast, protection of information in the nation is of immediate necessity according to many intellectuals and politicians[16] of Bangladesh since it is always possible that personal information of customers may always be given to the third parties without their prior consent. Moreover an individual may always feel that their personal data is being blandly misused and that their personal rights are being grossly violated. Therefore legal provisions are required to be made to protect the privacy of the people and deter them from committing such wrongful acts. A perception study stated that 40% of the respondents said that their privacy has been seriously threatened by the mobile phone companies in Bangladesh and 80% think that the preservation of their national identification card copies are not done in an appropriate manner.[17] It is necessary to mention that just keeping personal information secret is not all about Data Protection Law. It also demands the creation of a trusted framework for collection, exchange and use of personal data with regards to commercial and governmental contexts.[18]

Taking into consideration the Indian subcontinent, India has moved ahead for enacting a separate personal data protection law instead of making amendments to their Information Technology Act 2010[19] and it is high time that Bangladesh does the same. True, Asian counties have not yet given due importance to this matter. For instance, Malaysia does not have any clear laws that address data privacy nor does it adhere to international privacy agreements. On the other hand, many people think that Japan has most of the laws relating to privacy discussed in theory and the impact on actual practice is significantly low. South Korea is distinctive in Asia in the sense that it has a seemingly comprehensive privacy and data protection law. A 2004 bill aimed at ensuring that government at all levels can collect private information only with an individual's consent and this bill also specified that reasons for the collection of personal information must be stated clearly on concerned or relevant documents.[20]

IV. Laws Prevailing In Support Of Data Protection & Their Shortcomings

Despite the fact that there is no particular legislation for protection of personal data, however some safeguards can be formulated with respect to protecting privacy of an individual considering some existing laws and drawing examples from other developed and developing counties in the globe suited to conditions prevailing in Bangladesh.

"A representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored in the memory of the computer" is how Data is defined in accordance with the Information and Communication Technology Act 2006.[21] Although nowhere in the Act it includes the word 'personal data', the Act can still be used to protect personal data. A major section with relevance is Section 54 which foresees liability in case of data, computer database theft and may include the wide range of computer trespass, unauthorized digital copying, downloading and extraction of data, computer database or information. Also what it may cover is that theft of data held or stored in the media, unlawful transmission of data or program located in a computer, computer system or computer network. The section mentions that provided any person with no permission of the owner or any other person who is in charge of a computer, computer system or computer network, makes accesses or secures access to such computer, computer system or computer network, downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium or gets involved in damaging or causing damage to any computer, computer system or computer network, data, computer data base or any other programs lying in such computer, computer system or computer network, then the person shall be punishable with imprisonment for ten years, or with fine which may amount to Taka ten lakhs or both.[22] However the negative point lies in the fact that it states nothing with regard to personal data stored anywhere else but computers and about instances when the personal data may be taken illegally in any other form.

In Section 56 of the 2006 Act it is written that whoever having the intention to cause or knowing that he is likely to cause wrongful damage to the public or any person who destroys or alters any information stored in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking and shall be penalized.[23] However this section mainly deals with hacking. Lastly, Section 63 of the 2006 Act mentions about any person who, in pursuance of any of the powers conferred under this Act, or rules and regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material ,without the consent of the person concerned, discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be regarded as an offence and whoever commits any such offence shall be punishable with imprisonment for a term which may extend to two years, or with fine which may extend to Taka two lakhs, or with both.[24] Notably in Section 63, 'consent' of the concerned person is a must. However, it would be difficult to consider if it is capable of providing with a sufficient level of personal data protection.

Although in theory, law of tort provides with information privacy, in the case of Secretary General, Supreme Court of India v Subhash Chandra Agarwal, cause of action for damages resulting from illegitimate invasion of privacy for the first time was recognized.[25] Law of Tort can be said to be insufficient in providing with the concerned protection since there is no protection for personal information in public records, and protection of privacy for persons who have willingly placed themselves in the public eye is reduced in accordance with the case of Rajagopal alias Gopal v State of Tamil Nadu.[26]

Lastly, in accordance with the Contract Act 1872 if a party involves in committing a breach of contract, the other party shall be entitled to receive compensation for any loss or damage caused.[27] In some cases, the court may as well direct the "specific performance" of the contract against the party in default. Thus while getting into a contract; one may enter providing with a great level of personal data protection in paper since contracts are binding under the concerned Act. Thus Data Protection can be inserted into employment contracts and company policies.[28] But then again there would be problems if there is no contractual agreements between the parties or if one party does not agree to get into a contract to obey the 'protection of personal data' part.

V. Principles For The Enactment Of Data Protection Laws & Rights Thereof

For the purpose of protection of personal data, eight principles[29] can be taken into consideration. These are basically the main principles mentioned in the Data Protection Act 1998 of the United Kingdom. The principles explained in the following may be used as the basis for the enactment of a personal data protection law in Bangladesh, meaning that the law should be done with adherence to the guiding principles.

Fairly & lawfully processed – A person providing with the data will have to be informed that their data is being collected, their information is held by who and the specific individual controlling it, for what reasons the data will be used, exact span of time the data is going to be kept and if information will be provided to any third party.[30] Meaning that there should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, of course, with the knowledge or consent of the data subject.[31] The need for processing personal data fairly and lawfully is given out in this first data protection principle because processing personal data above everything else is a must to be fair, as well as having substantial and appropriate conditions for such processing. Provided any aspect of processing is not fair, there will be a breach of the first data protection principle. Fairly and lawfully means in the first place the data controller (who is the person deciding on the purpose for which) and the manner in which the data are processed have to comply with the common law of duty of confidentiality and there is a legitimate reason to process personal data. Secondly, the data subject (in case of a living individual to whom the data is related) is needed to understand and has to agree to who will process the data, how such is going to be processed and to what extent and for what purpose. Thirdly, the data should be taken in a manner that it is neither misleading nor deceiving and lastly whether it is justified by a legal or statutory requirement or significant to public interest, the processing of data subject information is only justified by informed consent.[32]

Processed for limited purposes – A person gathering the data has to be clear of his/her purpose of collecting the data. He/she may take responsibility to give privacy notices while collecting their personal data.[33] Meaning that Personal data should be relevant to the purposes for which they are to be used, and to the extent necessary for those purposes. The data has to be obtained only for one or more specified and lawful purposes, and should not be further processed in any manner incompatible with that purpose or those purposes.[34] This second data protection principle means that one must be clear from the outset about why one is collecting personal data and what one intends to do with it. This requirement (the second data protection principle) aims at ensuring that organizations are clear about their reasons for obtaining personal data, and that what they do with the information is in line with the reasonable expectations of the individuals concerned. Furthermore this principle intends to make the processing of personal data more transparent for the data subject and restricts the data controllers processing of personal data by limiting it to the specific purpose. The disclosure of personal data has to be compatible with the purpose for which the data subject has declared them originally. In other words, the confidential information obtained for one purpose cannot be used for any other purpose.[35]

Adequate, relevant and not excessive – Institutions or organizations should not collect data which are not strictly necessary.[36] One should hold personal data about an individual to an extent it is sufficient for the purpose of holding it and should not hold more information than necessary. This is part of the practice is known as "data minimization".[37] It won't, therefore be acceptable to hold information on the basis that it might possibly be useful at some point time in the future without a clear view of how it will be used.[38] The data controller should not hold more personal data than is necessary nor should the data he holds include irrelevant details. In case of sensitive personal data, it is particularly important to make sure that only minimum amount of information is obtained. If it is necessary to hold particular information about certain individuals only, then it

should be collected in adherence to the principles. Otherwise the information is likely to be excessive and irrelevant in relation to other people.[39]

Accurate and up-to-date –At least once a year, it should be checked if files are accurate and updated. This can be done by conducting an information audit.[40] For instance, if an individual has shifted residence from Sydney to Melbourne, a record showing that he or she is currently living in Sydney is certainly inaccurate. But a record showing that he or she once lived in Sydney remains accurate, despite the fact that the person no longer resides there. If information is used for a purpose that relies on it remaining current, it should be kept up-to-date. Another instance, when there is a pay-rise; employee payroll records should be updated. Likewise, records should be updated for customers' change of address so that goods are delivered to the correct geographical location.

Not kept longer than necessary - This principle mentions regarding the span of time for which the information is essential in order to perform the operation for which it was collected.[41] This principle basically states that the length of time that personal data is kept should be reviewed to consider the purpose or purposes for which the information is held for deciding whether (and for how much span of time) to retain it any longer. The information that is no longer needed should be securely deleted or archived if the information goes out of date. For instance, considering a bank that holds personal data about its customers, the personal information it holds includes details of each customer's address, date of birth and mother's maiden name etc. The bank uses this information as part of its security procedures. It is applicable for the bank to retain this data for as long as the customer has an account with the bank and no longer. However, even after the account has been closed, the bank may require keeping on holding some of the given information for legal or operational purposes only. The present and future value of the information, the costs, risks and liabilities related to retaining the information and the reasonable difficulty of making sure it remains accurate and up-to-date determines the length of retaining data.[42]

Processed in line with the Data provider's rights - There are important privacy rights mentioned in legal provisions including confidentiality under common law and rights in the Human Rights[43] Law.[44] This principle states the rights of the individuals namely, a right of access to a copy of the information comprised in their personal data, a right to object to processing that is likely to cause or is causing damage or distress ,a right to prevent processing for direct marketing, a right to object to decisions being taken by automated means, a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed and a right to claim compensation for damages caused by a breach of the Act.[45] The "right to prevent processing may give the impression that an individual can simply demand that an organization stops processing personal data about them, or stops processing it in a particular way, the right is often overstated. In practice, it is much more limited. An individual has a right to object to processing only if it causes unwarranted and substantial damage or distress. An individual should have the right to obtain from a data controller, confirmation of whether or not the data controller has data relating to him and to have communicated to him, data relating to him within a reasonable time. He should also have the right to challenge data relating to him and, if the challenge is valid, to have the data erased, rectified, completed or amended.[46]

Securely kept - This principle requires that technical and organizational measures have to be taken against unlawful access to personal data and against accidental loss or destruction of personal data. Meaning that personal data should not be disclosed, made available or otherwise used except with the consent of the data subject or by the authority of law.[47] Information security breaches may cause harm and distress to the individuals they affect; it may also turn out to be risky for many lives. Examples of the harm caused by the loss or abuse of personal data (sometimes linked to identity of fraud) include: fake credit card transactions, witnesses at risk of physical harm or intimidation, offenders at risk from vigilant, exposure of the addresses of service personnel, police and prison officers, and women at risk of domestic violence. Fake applications for tax credits and others are also a matter of concern.[48] Not all security breaches have such grave consequences, of course. Many cause less serious embarrassment or inconvenience to the individuals concerned. Individuals are entitled to be protected from this kind of harm as well. Advances in technology have enabled organizations to process more and more personal data, and to share information more easily. This has obvious benefits if they are collecting and sharing personal data in accordance with the data protection principles, but it also gives rise to equally obvious security risks. The more databases that are set up and the more information are exchanged, the greater the risk that the information will be lost, corrupted or misused.[49]

Accountability - A data controller should be accountable for complying with measures which give effect to the principles stated above. This principle has to limit transfer of personal data within a particular territory - risk issues considering transfer of personal data unless the nation has sufficient level of protection.[50] Before making a transfer, one should take into consideration whether he or she can achieve his/her aims without actually processing personal data. For example, if data is made anonymous so that it is not possible to identify individuals from it, now or at any point in the future, then the data protection principles will not apply and he/she is free to transfer the information.[51]

Concerning the above principles, Rights to be provided under the recommended Act can be well specified. One of such can be the right which would allow one to look for what information is held about him/her. Person holding the data may be prevented from processing ones information to avoid causation of unjustified damage or suffering of possibly anyone at all. One may ask for a copy of all his or her personal details by writing to any organization or person holding these details on a computer or in manual form. He or she may also ask the data controller to inform of any opinions given about him/her, unless the data controller considers that the opinions are confidential.[52]

Even in such cases, his/her right to such information will usually be greater than the right of the person who gave this opinion in private. This right does not apply, however, in a small number of cases where it could harm certain interests – for example when someone is investigating an offence. One should also be informed of, and given the chance to object to, any decisions about he/she that are automatically generated by a computer without any human involvement. If one discovers that a data controller has details about his/her that are not factually correct, one can ask them to change or, in some cases, remove these details. If one feels that the organization or person does not have a valid reason for holding his or her personal details or that they have taken these details in an unfair manner, he/she can ask them to change or remove these details. In both cases, he or she may write to the organization or person, explaining your concerns or outlining which details are incorrect. Considering direct marketing, person providing the data should be able to stop relevant activities. Meaning that, individuals can ask the Data Controller at any time not to use their personal information for direct marketing purposes. They may consider making their request in writing and the Data Controller must act on it in a reasonable period of time. In such cases, this should be within a month or so.

Existence of an Act would further give rights of claiming compensation in case of breach. One may apply to the court to order a data controller to rectify, block or destroy personal details provided there is any inaccuracy or if it contains expressions of opinion based on inaccurate information. Meaning that an individual should have the right to have incorrect or misleading personal information held about them corrected. If the data controller does not do this, they could obtain a court order directing you to correct, delete, block or destroy the information. If this happens, it will be up to the court to decide if the information is inaccurate and what (if anything) to do about it. The individual may also ask the court for compensation and costs. A body/commission in control of organizations or individuals holding data should take complaints from the persons who provide information against the ones holding such. In order to make a complaint, one may simply write to or email the Data Protection Commissioner explaining his/her case. In your letter or email, one should name the organization or person complained about, describe the steps he/she has taken to have the concerns dealt with, provide with details of any response which he/she had received and be sure to provide copies of any letters or emails exchanged between him/her and the organization or person.[53] It would be duty of the Commissioner to investigate the complaint and try to resolve the matter in the best way possible. If this is not possible, one may ask the Commissioner to make a formal decision on whether the data controller has violated his/her rights. However, the Commissioner may not be able to award you compensation. If the Commissioner agrees with the complaint, he will try to make sure that the data controller obeys the law and puts matters right. If the Commissioner rejects the complaint, he will let the person know in writing. If one is not happy with the Commissioner's decision, he/she can appeal the decision in the Circuit Court.[54]

VI. Personal Data Protection Law In Line With The Constitution & Recommendation

Personal data protection laws definitely fall within the area of right to privacy. Meaning that unlawful use of personal data basically means violation of the person's privacy. However with respect to right to privacy, even the developed United States does not contain explicitly the right to privacy.[55]

Considering the Constitution of the People's Republic of Bangladesh, PART III provides that 'no person shall be deprived of life or personal liberty except according to procedure established by law'.[56] Judicial intervention is very much possible in the legal system of Bangladesh and so despite the fact that privacy issues does not include the matter of data protection explicitly, yet case principles may be taken into consideration.

In the case of Kharak Singh v The State of U.P. the Supreme Court of India concluded that the Article 32 of the Constitution includes "right to privacy" as a part of the right to "protection of life and personal liberty". The Court paralleled 'personal liberty' with' privacy', and mentioned that the concept of liberty in the Constitution was wide-ranging enough for the inclusion of privacy in it. Moreover in District Registrar and Collector v. Canara Bank, the Supreme Court of India mentioned that an individual's right to privacy exists and any illegitimate invasion of privacy would make the person committing an offence responsible for the consequences with reference to the law and that there is also constitutional recognition given to the right of protecting personal privacy against illegal governmental invasion.[57]

In the case of R. Rajagopal v State of Tamil Nadu, it was held that the petitioners have a right to publish what they allege to be the life story/autobiography of Auto Shankar in so far as it appears from the public records, even without his consent or authorization. But if they go beyond that and publish his life story, they may be invading his right to privacy, and then they will be liable for the consequences in accordance with law.[58] A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child bearing and education among other matters. No one has the rights to publish anything concerning the above matters without the person's consent, despite the information being true or false and whether complimentary or critical. Provided someone does so, he or she would be violating the right to privacy of the person concerned and would be liable for an action for damages.[59] One other case where right to privacy is stated is People's Union for Civil Liberties (PUCL) v Union of India which held that the telephone tapping by Government amounts to infraction of personal liberty of the Constitution of India. Right to privacy is a part of the right to "life" and "personal liberty" enshrined under the Constitution. The said right cannot be curtailed "except according to procedure established by law".[60] As mentioned already, the above are just some case principles adding to the basics of formulating a law regarding right to privacy.

Furthermore, in Article 39 (Right to freedom of thought, conscience and of speech)[61] and Article 36 (Right of freedom of movement)[62] of the Constitution, it is a requirement that Privacy is to be protected and these article permits the State to impose reasonable restrictions on the exercise of the rights conferred by them in the interest of the sovereignty and integrity of Bangladesh, the security of the State, friendly relations with foreign States, public order, decency, morality, contempt of court, defamation and incitement of offence.[63] However a point to be taken into consideration is that Article 39 of the Constitution guarantees to all citizens 'freedom of speech and expression', thus meaning that these have to be balanced. Again in India, the Supreme Court has held in the case of State of U.P. v Raj Narayan that a citizen has a right to receive information derived from the concept of freedom of speech and expression.[64] The legal system of Bangladesh is open to judicial intervention, despite the fact that the cases on privacy issues have not yet involved data protection issues till date.

So provided a personal data protection law is formulated, the terms 'personal data' and 'sensitive personal data' are required to be defined in easy and clear language. Furthermore, the parties concerned must be mentioned as well. For instance 'Data Subject' is the person whose data is being processed.[65] For example, the student who provides with his full name, gender, address, phone number etc for admission in a high school, the 'Data Controllers' will control the contents and use of personal data. Data Controllers can either be legal entities such as companies or government departments or public authorities or even individuals like sole-traders.[66] In addition, there are Data Processors or Assistants who process the data on behalf of the Data Controller.[67] For example, employee(s) of the Data Controller.

The Data Controllers should be well aware of the responsibilities they are going to have regarding protection of personal data. It is important that they make aware their employees aware regarding the concerned providing them with training or providing them with the policies. Data Controllers are required to inform the individual who provided with data (Data Subjects) about the purposes of the processing. Such information may be provided in the form of a data protection notice such as the details of the data controller; the purposes for the processing, including any non-obvious purposes like cross-mailing or host mailing, details of any recipients of the personal data. For example, other companies within the group and their purpose. An opt-out/ opt-in to marketing, as appropriate, an explanation of the methods to be used for contacting individuals for marketing purposes. For instance telephone can be used. Other options are fax, SMS, email etc. They should provide with any other information that is necessary to make the processing fair.[68]

The legal provision should also provide that the personal data of any person collected for a particular purpose or obtained in connection with any transaction, whether by appropriate government or by any private organization, shall not be put to processing without the consent of the person concerned but that personal data of any person may be processed without consent for the prevention or detection of crime, the prosecution of offenders, the assessment or collection of any tax or duty and if the personal data details of the individual are obtained through sources which have been made public.

There should also be a provision where the controller is liable to provide, free of charge, concerning whether personal data relating to a particular person has to be processed or not, provided the person so desires. If such data is processed, written information should be provided about where the data has been collected from the purpose of the processing and to which recipient or categories of recipients the data is being disclosed. The information should be provided within a prescribed period from when the application was made.[69] The controller is going to be liable, upon request, by the registered person, to correct, block, restrict or erase them as soon as possible, if such personal data are incorrect.

The Personal Data Protection Laws should also imply that the controller is liable to implement technical and organizational measures to protect the personal data. The measures shall attain a suitable level of security.[70] When the controller engages an assistant to conduct the processing of personal data, there shall be a written contract that specifically regulates the security aspects. The controller shall also be responsible to ensure that the assistant actually implements the necessary security measures. If someone who works for the controller discloses personal data in contravention of that provided by the Personal Data Act, it is the controller who bears the legal responsibility in relation to the registered person.[71]

The law should also provide that any person who commits fraud or causes unauthorized disclosure of personal information or contravenes in any of the above provisions should be penalized with fine and imprisonment or both. It shall also provide that any person who has intentionally or by gross negligence disclosed untrue data information or notifications or who in contravention of the provisions processes sensitive personal data or data concerning offences, or transfers personal data to a third country which doesn't have data protection laws or neglects to give notice concerning the processing to the supervisory authority may be sentenced to a fine or imprisonment.

In cases Data Controllers do not comply with the rules or whatever is right for them to do, an inspection board or a commission is required that would inspect personal data situations surrounding the processing for the purpose of assessing whether or not any processing of the data is carried out in compliance with the law that is to be made. The commission/board may also ask for reports from the Data Controllers.[72] Non-compliance with the law should amount to criminal liability as well which does not necessarily have to lie just with the data controller. It is possible for directors/managers of a company to be personally criminally liable if the offence is committed with their consent, involvement or neglect. Employees may also incur criminal liability in certain circumstances if they disclose or obtain personal data without authority of the data subject controller.[73]

VII. Conclusion

For reasons that Bangladesh is not having any laws for the protection of personal data, the information collected by different organizations are often abused or misused, eventually leading to the suffering of individuals. For instance, personal information of an individual collected for a particular purpose is commonly misused for other purposes, like direct marketing without the consent of the individual. Some internal confidentiality standard within the system is required so that personal information of an individual does not get transferred to others easily causing irreparable distress or embarrassment. Despite inclusion of right of privacy, the Contract Law and the Law of Tort and specifically the Information and Communication Technology Act, the arena covered leaves much more to be desired. Therefore Bangladesh requires to enact a full-fledged law which should be detailed enough to meet the international standards for protection of personal information and ensure that personal information of an individual collected for a particular purpose should be used for that particular purpose and it would not be revealed or divulged to others for commercial or any other purposes. Therefore, the law to be enacted should mention appropriate definition of personal data, limitations for the usage of data, what penalty should be imposed for the non-compliance and remedies to be specified, considering misuse of data and keeping the data safe for the best interest of the citizens of the country at large. Anything short of that would be a wanton denial and fair play a civilized society or country should always deserve. It is high time that the government of Bangladesh goes for enactment of the laws for protection of personal data – the sooner it is done, the better.

Acknowledgement

We gratefully acknowledge the support and generosity of Dr. Md. Rizwanul Islam, a recipient of the Macquarie University Research Excellence Scholarship, and our Legal Research course faculty during our LL.B.(Hons.) at BRAC University, Bangladesh.

References

[1]. M. Zamir, 'The collection, sharing and projection of data', *The Daily Star (Dhaka)*, 31 May 2008, 2.
[2]. European Commission, Why do we need data protection rules now (25 January 2012) New Data protection rules for the digital age <http://ec.europa.eu/justice/data-protection/minisite/>.
[3]. P Diwan and S Kapoor, *Cyber and e-commerce laws*, (Bharat Publication, 2nd Ed, 2000) 4.
[4]. Freedom of Speech, The EU Data Protection Directive and the Swedish Personal Data Act (9 June 2000) History <http://people.dsv.su.se/~jpalme/society/eu-data-directive-freedom.html#EU>.
[5]. Northumbria University,History Of Data Protection Legislation <http://lawresearch.northumbria.ac.uk/cirl/sources/dpa/history/?view=Standard>.
[6]. Sharad Vadihera,'Data Protection and Information Technology Act in India' on Global Advertising Lawyers Alliance <http://www.gala-marketlaw.com/joomla4/index.php?option=com_content&view=article&id=261&Itemid=138>.
[7]. G Greenleaf, Promises and Illusion of Data Protection in Indian Law, Oxford Law Journal 47(1).
[8]. Data Protection Act 1988 (UK) s 1(1). ('UK Data Act').
[9]. R Morgan and R Boardman, *Data Protection Strategy – Implementing Data Protection Compliance* (Sweet and Maxwell Limited, 1st Ed, 2003) 5.
[10]. Hammonds, *Data Protection* (Chartered Institute of Personnel & Development, 2nd Ed, 2004) 6.
[11]. Standard Chartered Bangladesh, Data Protection & Privacy Policy <http://www.standardchartered.com/bd/data-protection-privacy-policy/en/>.
[12]. Bangor University, What is Data Protection <http://www.bangor.ac.uk/ar/ro/recordsmanagement/dataprotection/whatis.php.en>.
[13]. Hammonds, *Data Protection* (Chartered Institute of Personnel & Development, 2nd Ed, 2004) 9
[14]. JISC Legal Information, Data Protection Overview (27 August 2007) <http://www.jisclegal.ac.uk/LegalAreas/DataProtection/DataProtectionOverview.aspx#_Toc174939787>.
[15]. Information and Communication Technology Act 2006 (Bangladesh) sub-s s 7(h), (i), (j), (r). ('2006 Act').
[16]. Farjana Akter, 'Speakers demanded privacy and data protection laws in national convention' on Voices for Interactive Choice & Empowerment (14 February 2012) <http://www.voicebd.org/node/361>.
[17]. Farjana Akter, 'Call to Observe International Privacy Day: Data protecton law to secure personal information' on Voices for Interactive Choice & Empowerment (27 January 2012) <http://www.voicebd.org/node/359>.
[18]. Legal Service India, Data Protection Laws in India-Needs and position (22 July 2009) <http://www.legalserviceindia.com/article/l368-Data-Protection-Law-In-India.html>.
[19]. Final Analysis of Data Protection Law in India <http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_india_en.pdf>.
[20]. [20] Simson Garfinkel and Beth Rosenberg, RFID,Applications,Privacy,Security (Pearson Education, 1st Impression, 2006) 454.
[21]. 2006 Act s 2(10).
[22]. 2006 Act s 54.
[23]. 2006 Act s 56.
[24]. 2006 Act s 63.
[25]. Secretary General, Supreme Court of India v Subhash Chandra Agarwal [2010] INHCD 40[110]
[26]. Rajagopal alias Gopal v State of Tamil Nadu [1994] 6 SCC 632
[27]. The Contract Act 1872 (Bangladesh) s 73.
[28]. Practical Law Company, Doing Business in Bangladesh (1 October 2010) <http://crossborder.practicallaw.com/1-504-7011?q=*&qp=&qo=&qe>.
[29]. Data Protection Act : Explained <http://dataprotectionact.org/1.html>.
[30]. JISC Legal Information, Data Protection Overview (27 August 2007) <http://www.jisclegal.ac.uk/LegalAreas/DataProtection/DataProtectionOverview.aspx#_Toc174939787>.
[31]. Data Protection Law in India <http://www.naavi.org/cl_editorial/edit_25may_02_1.html>.
[32]. Tobias Keyser and Christine Dainty, The Information Governance Toolkit: Data protection, Caldicott, Confidentiality (Redcliffe Publishing, 1st Ed, 2005) 96.
[33]. Information Commissioner's Office, Processing Personal Data for Specified Purposes <http://www.ico.gov.uk/for_organisations/data_protection/the_guide/principle_2.aspx>.
[34]. Information Commissioner's Office, Processing Personal Data for Specified Purposes <http://www.ico.gov.uk/for_organisations/data_protection/the_guide/principle_2.aspx>.
[35]. Tobias Keyser and Christine Dainty, The Information Governance Toolkit: Data protection, Caldicott, Confidentiality (Redcliffe Publishing, 1st Ed, 2005) 98.
[36]. School of Oriental and African Studies, Data Protection Policies: Overview of the Data Protection Act 1998 (December 2007) <http://www.soas.ac.uk/infocomp/dpa/policy/overview/>
[37]. School of Oriental and African Studies, Data Protection Policies: Overview of the Data Protection Act 1998 (December 2007) <http://www.soas.ac.uk/infocomp/dpa/policy/overview/>
[38]. Tobias Keyser and Christine Dainty, The Information Governance Toolkit: Data protection, Caldicott, Confidentiality (Redcliffe Publishing, 1st Ed, 2005) 99.
[39]. Tobias Keyser and Christine Dainty, The Information Governance Toolkit: Data protection, Caldicott, Confidentiality (Redcliffe Publishing, 1st Ed, 2005) 99.
[40]. Tobias Keyser and Christine Dainty, The Information Governance Toolkit: Data protection, Caldicott, Confidentiality (Redcliffe Publishing, 1st Ed, 2005) 99.
[41]. JISC Legal Information, Data Protection Overview (27 August 2007) <http://www.jisclegal.ac.uk/LegalAreas/DataProtection/DataProtectionOverview.aspx#_Toc174939787>.
[42]. Rolf Hernegran, Personal Data Protection Law (Regeringskansleit, 4thEd. ,2006) 15.
[43]. Human rights act 1998 (UK) art 8.
[44]. The Rights of Individuals <http://www.ns/data_protection/principle_6.aspx>.
[45]. The Rights of Individuals <http://www.ns/data_protection/principle_6.aspx>.
[46]. M.s Siddiqui,'Privacy Act Vs. Right to Information Act' The Financial Express (Dhaka), 10 June 2011, 3[3].
[47]. JISC Legal Information, Data Protection Overview (27 August 2007) <http://www.jisclegal.ac.uk/LegalAreas/DataProtection/DataProtectionOverview.aspx#_Toc174939787>.
[48]. The Rights of Individuals <http://www.ns/data_protection/principle_6.aspx>.

[49]. Information Security <http://www.icoorganisations/data_protection/information security/principle_7.aspx>.
[50]. JISC Legal Information, Data Protection Overview (27 August 2007) <http://www.jisclegal.ac.uk/LegalAreas/DataProtection/DataProtectionOverview.aspx#_Toc174939787>.
[51]. Rolf Hernegran, Personal Data Protection Law (Regeringskansleit, 4thEd. ,2006) 24.
[52]. Business link,Comply With Data Protection Legislation < http://www.businesslink.gov.uk/bdotg/action/detail?itemId=1074414316&type=RESOURCES>
[53]. Information Commissioner, Data Protection Act: your Righs and how to Enforce them < http://www.article12.org/pdf/data%20protection%20act%20your%20rights.pdf>
[54]. Information Commissioner, Parliament of UK, Data Protection Act Factsheet (1998) 2.
[55]. Harry Browne, Does the Constitution Contain a Right to Privacy? (9 May 2003) < http://harrybrowne.org/articles/PrivacyRight.htm>
[56]. The Constitution Of India 1949 (India) art 32
[57]. District Registrar and Collector v. Canara Bank [2005] 1 SCC 496.
[58]. R. Rajagopal v State of Tamil Nadu [1995] AIR 264 (SC)
[59]. R. Rajagopal v State of Tamil Nadu [1995] AIR 264 (SC)
[60]. People's Union for Civil Liberties (PUCL) v Union of India [1997] 1 SCC 301.
[61]. M.A.Salam, The Constitution of the People's Republic of Bangladesh (CIJ, 1st Ed, 2003) art 39
[62]. M.A.Salam, The Constitution of the People's Republic of Bangladesh (CIJ, 1st Ed, 2003) art 39
[63]. M.A.Salam, The Constitution of the People's Republic of Bangladesh (CIJ, 1st Ed, 2003) art 39(2)
[64]. State of U.P. v Raj Narayan [1975] AIR 86 (SC)
[65]. Hammonds, Data Protection (Chartered Institute of Personnel & Development, 2nd Ed, 2004) 11.
[66]. Data Protection Commissioner, A Guide for Data Controllers <http://www.dataprotection.ie/docs/a_guide_for_data_contollers/696.htm>.
[67]. Rolf Hernegran, Personal Data Protection Law (Regeringskansleit, 4thEd. ,2006) 11.
[68]. Out-Law, Data Protection <http://www.out-law.com/page-413>.
[69]. Rolf Hernegran, Personal Data Protection Law (Regeringskansleit, 4thEd. ,2006) 20.
[70]. Rolf Hernegran, Personal Data Protection Law (Regeringskansleit, 4thEd. ,2006) 23.
[71]. Rolf Hernegran, Personal Data Protection Law (Regeringskansleit, 4thEd. ,2006) 23.
[72]. Data Protection Powers and Penalties <http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/data_protection_powers_penalties_v1_dec07.pdf>5.
[73]. Data Protection Powers and Penalties <http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/data_protection_powers_penalties_v1_dec07.pdf>5.