Daily Star, 15 December 2017

RTI vs RTP: Is there a contradiction?

Shamsul Bari and Ruhi Naz

The disclosure of information on people's race or ethnicity during World War II caused one of the worst tragedies known to mankind. It led to secret denunciations and seizures, sending millions of friends and neighbours to labour and concentration camps and eventually to gas chambers. It changed the course of history.

A fundamental change it gave rise to was elevating the status of the individual vis-à-vis the State. It led to the introduction of Europe's stringent privacy regulations. Governments in Europe took steps to protect personal information of individuals from such abuses in the future. The concept of protection of personal data or privacy was born. It spread all over Europe quickly, and to the rest of the world gradually.

The technological inventions of our time, including the Internet and social media, have enabled unprecedented connectivity in the world. While humankind is ever closer, privacy and personal space for individuals is constantly shrinking.

The definition of privacy and the meaning of sensitive personal information vary among countries and cultures. Some cultures focus more on community rights rather than individual rights; others, such as countries in Europe, are sensitive to privacy rights because of their experiences in the World War II era.

However, the legal right to privacy is recognised in nearly every national constitution, as in ours, and in most international human rights treaties including the Universal Declaration of Human Rights.

Common examples of “personal data” are: address, credit card number, bank statements, criminal record, medical record, etc. However, new technologies have driven the collection of personal information by governments and private bodies far and wide. Databases handling information that range from tax, medical, employment, criminal, and citizenship records to identification technologies such as identity card systems, fingerprints, and DNA mapping, proliferate at a faster pace. Services run by communications operators collect information such as emails, records of persons communicated with, lists of websites visited, and mobile locations. And, of course, people share information through social networking sites.

The increased flow of personal data across borders has caused growing concerns among citizens about data abuse by governments and private bodies. There are increasing calls from citizens' groups all over the world for their protection. What is our perspective on the matter in Bangladesh?

Some 80 countries all over the world have adopted comprehensive laws that give individuals some control over the collection and use of these data by public and private bodies. They are among 115 countries that have also legislated on citizen's right to information held by governments.

On the face of it, the right to information (RTI) and the right to privacy (RTP) may appear irreconcilable. RTI laws empower citizens to access information held by governments and public bodies. RTP laws, on the other hand, grant individuals a fundamental right to control the collection of, access to, and use of personal information that is held by governments and private bodies. Thus, one promotes access and the other seeks to control it.

However, instead of looking at them as conflictual laws, RTI and RTP are better considered as “two sides of the same coin.” They complement each other in the sense that one promotes individuals' right to protect themselves and the other promotes government accountability. Both are essential for good governance. This explains why there is considerable debate around the globe on the subject. Is there a need to adopt both the laws or a single law can cover both?

In Bangladesh, unlike in most industrialised countries, there is no single specific privacy or personal data protection law. The Constitution and other laws of the land, however, provide some protection. For example, Article 43 of the Constitution recognises the right of every citizen to be secured in his/her home against entry, search and seizure (subject to any reasonable restrictions imposed by law in the interests of the security of the State, public order, public morality or public health). It also recognises the privacy of a citizen's correspondence and communications.

The RTI Act also provides protection of personal information that may offend the privacy of the personal life of an individual—and any such information that may endanger the life or physical safety of any person.

Additionally, the Information and Communication Technology Act 2006 provides for safeguards of information and related matters stored in the memory of the computer. Although the Act does not explicitly mention “personal data,” there is scope for implied use. An area of relevance is Section 54, which foresees liability in case of data, computer database theft and a wide range of computer trespass, unauthorised digital copying, downloading and extraction of data, computer

database or information. To the extent they may relate to personal information or data, they are of relevance. Stiff punishment has been provided for any infringement. However, the provision does not extend to personal data stored anywhere else other than in computers.

The law of tort may also be of some use for protection of personal data. Damages may, for example, be sought for illegitimate invasion of privacy. The Contract Act 1872 may similarly provide protection in the form of compensation or damages if a party breaches a contract. For example, personal data protection can be inserted into employment contracts and company policies.

But these are not enough in the current data privacy context. As a fast-developing country, we certainly need a broader personal data protection regime to cover all the contingencies. Guidance in this regard is available from the most influential of all Data Protection instruments of the world, the European Union (EU) Data Protection Directive. It has been adopted by the 27 EU member-states (plus three European Economic Area countries) and by numerous other countries in Africa, Europe, and Latin America that trade with the EU.

The directive takes a broad approach to personal information. Personal data are defined as “any information relating to an identified or identifiable natural person... one who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.”

The UK, too, has a Data Protection Act in addition to the Freedom of Information Act (FOI). While the FOI applies only to public sector organisations, it covers a wide range of information. The Data Protection Act, which applies equally in both the public and private sectors, allows individuals the right to find out what information about them was being held, and to insist on having that information kept accurate and up-to-date. The UK Information Commissioner's office deals with dispute resolution for both the instruments.

In the US, though there is no single data protection law comparable to the EU's Data Protection Directive, there are many privacy legislations adopted on an ad hoc basis, as and when circumstances require (e.g., the Video Privacy Protection Act of 1988, the Fair Credit Reporting Act, and the 1996 Health Insurance Portability and Accountability Act).

The above may provide us with guidelines on how to go about the subject in Bangladesh. It is up to us now to decide what is best for us. Do we need separate privacy legislation, as in EU countries, or should we be satisfied with ad hoc mechanisms, as in the US? The Government may have some ideas on the subject but since the subject of privacy concerns citizens directly, we must take the lead. Is the civil society in Bangladesh ready for this challenge?

Dr Shamsul Bari and Ms Ruhi Naz are Chairman and Coordinator (RTI) respectively of Research Initiatives, Bangladesh (RIB).
Email: rib@citech-bd.com