Implication of Law and Governance in Enhancing Information Security in Digital Era

S. Kandasamy
Associate Professor, Department of Public Policy, Law and Governance, Central University of Rajasthan, Bandarsindri-305817, Ajmer, Rajasthan State, India

Abstract

Governance focuses on administrative efficiency and accountability – Governance is not only limited to Government agencies, it is extended to NGO and Self Help Groups also – Information is an essential factor of decision making – Information and Communication Technology facilitates the effective Governance – Hence, there is requirement of Information Security.

Government requires sensitive information for decision making process – Information shall be secured – Electronic record, Electronic evidence and Electronic information are part of Governance Process – Law regulates all these aspects of information – Information Technology Act plays a key role in protecting electronic information.

Information security is ensured under Information Technology Act – For breach of security, law imposes punishment also – Information is authenticated through the mechanism of Digital Signatures.

Information security is ensured through International Law also. Convention on Cybercrimes deals with the international aspect of cybercrimes – Many countries have enacted cybercrimes Acts also- India also included the provisions related to cybercrimes under Information Technology Act.

Implementation mechanisms on cyber security have also been established in India like that of Digital Signature Authority and Computer Emergency Response Team – But still the information security could not be achieved upto the desired level.

KEYWORDS: Good-Governance, E-Governance, Information Security, Information Technology, International Law and Cybercrimes.

Introduction:

Governance is basically concerned with administrative efficiency and accountability. But it may involve concerns to democracy, human rights and participation. Now, it is recognized that Governments are not the whole guardians of power and welfare to people. It is shared with Government organs, civil society, NGOs and Self Help Groups (SHG) and so on.

Access to Information and Knowledge forms the basis of decision making. Well informed

Decision-making is dependent on the quality and timeliness of information. This is equally applicable in judicial decision making. Good governance is a part of a developmental process which is participatory, transparent and accountable. E-Governance facilitates good governance. E-Governance is much more massive transformation than electronic delivery. The basis of e-governance strongly rooted in the information technology. It pervades the process of judicial decision making and depends on the timely information. For executives it is a tool for good governance.

Information and Communication Technology can help governance to create awareness and opportunities to enable people participate in the governance process through:-

(i) Issues and agendas would be part of the larger public debate before any decision is taken on them.
(ii) Expanding policy debates beyond the confines of dominant individuals and groups, and enriching the stock of policy knowledge in the process.
(iii) Greater transparency in actions and decisions.
(iv) Creation of public watch guards.
(v) Creation of strong virtual communities.
(vi) Online polls.
(vii) Grater representation of an un-represented communities i.e., women and aged children who are otherwise kept marginalized out of democratic process.

As a model, United Nations Development Programme is using Information and Communication Technology to:-

(i) Raise awareness, build vision and advise on policies to capture information and knowledge for development.
(ii) Promote and built connectivity and necessary infrastructure for access to information and development.
(iii) Build required human and social capacities and institutions and provide training and education to impart requisite skills.

E-Governance and Information Security:

Government being the prime custodian of the sensitive information, and being the largest business entity of any nation may suffer from unwanted perforation due to e-government.[1] U.S.A has a pretty stable and an extremely good infrastructure for e-governance. South Africa is in moderate category and India is in initial stages of implementing the e-government. U.S.A enacted E-Governance Act, 2002 to deal with the aspects of e-governance there. Title III of the Act [2] deals with Information Security. Purposes of Information Security [3] under the Act are:

(i) Provide a comprehensive framework for ensuring the effectiveness of information security, controls over information resources that support Federal Operations and assets;
(ii) Recognize the highly networked nature of current federal computing environment and provide effective government wide management and oversight of the related information security risks, including co-ordination of information security efforts throughout the civilian, national security and law enforcement communities;
(iii) Provide for development and maintenance of minimum controls required to protect Federal Information and Information Systems;
(iv) Provide a mechanism for improved oversight of Federal Agency Information Security Programs;
(v) Acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions reflecting market solutions for the protection of critical information infrastructures important to the national defence and economic security of the nation that are designed, built, and operated by the private sector; and
(vi) Recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.

In India also beyond the incorporation of the provisions in Information Technology Act, 2000, many other enactments are also amended so as to include electronic record, electronic evidence and electronic information.[4]

Under the Indian Evidence Act also the related provisions are amended to include electronic evidence.[5] Amendments to the Bankers Books Evidence Act, 1891 and Reserve Bank of India Act, 1934 were also amended to include electronic record, storage devices and print out.[6]

Electronic Communications and Transaction Act, 2002 (South Africa) protects personal information as well as critical database.[7]Theprinciples involved in collecting of personal information are:-

(i) A data controller must have the express written permission of the data subject for the collection, collation processing or disclosure of any personal information on that data subject unless he or she is permitted or required to do so by law.

(ii) A data controller may not electronically request, collect, collate, process or store personal information on a data subject which is not necessary for lawful purpose.

(iii) The data controller must disclose in writing to the data subject the specific purpose for which any personal information is being requested, collected, collated, processed or stored.

(iv) The data controller may not use the personal information for any other purpose than the disclosed purpose.

(v) The data controller may not disclose any of the personal information held by it to a third party unless required or permitted by law or specifically authorized by the person.

(vi) The data controller must delete or destroy all personal information which has become obsolete.

Information Security under IT Act:

Many of the copyright violations are treated as offences under Information Technology Act.[8] Further, the most of the offences under the Act have been made as both cognizable and non-bailable. Hacking, which is one of the main form of threat to information security is identified as[9] (a) whoever (b) with intention or knowledge (c) causing wrongful loss or damage to the public or any person (d) destroying any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means.

Hacking involves mental act with destructive animus. Hacking would mean destruction or alteration of any information residing in a computer resource, i.e., destruction or alteration of tangible and or intangible assets of a computer resource. The perspective of this provision is not to rarely protect the information residing in a computer resource but to protect the integrity and security of computer resources from attacks by unauthorized persons seeking to enter such resources, whatever may be their intention or motive.

Further, the idea behind the Act [10] is that the person who has secured access to any protected information shall not take unfair advantage of it by disclosing it to the third party without obtaining the consent of the disclosing party. An obligation of confidence arises between the data collectors and the data subject.

The Act prohibit the malicious publication of digital signature.[11] Publication is defined as the action of making publically known. The Supreme Court held in the case of Bennett Coleman & Co. v. Union of India[11] that publication means dissemination and circulation. In the context of digital medium, the term publication

includes dissemination, storage and transmission of information or data in the electronic form. Publishing the digital signature certificate for any fraudulent or unlawful purpose shall be punishable with imprisonment up to 2 years or fine of rupees one lakh or with both.[12]

Information Security and International Law:

The issue of Information Security has been on the UN agenda since the Russian Federation in 1998 first introduced a draft resolution.[13]The most recent resolution [14] of the UN General Assembly on the issue was adopted on 2nd Dec 2014. Information Society and Development Conference, [15] World Summit on Information Society [16] were held to make consensus on Information Security among the nation states. The goal of the world summit was to provide low-cost and high-impact training for the regional population in matters of security concepts and techniques, as well as policies, procedures, technology, education and awareness.

In early June 2012, St Petersburg hosted a third international meeting of high representatives in charge of security matter.[17]Further, UN General Assembly made a resolution [18] on the subject of 'Creation of a global culture of cyber security and taking stock of national efforts to protect critical information. The purpose is to identify the rights and responsibilities of states in information space, promote their constructive and responsible behaviour and enhance their cooperation in addressing common threats and challenges in information.

Council of Europe Convention on Cybercrime:

This convention was adopted in 2001. It created an international task force to oversee a range of security functions associated with internet activities for standardized technology laws across borders. It also attempts to improve the effectiveness of international investigations into breaches of technology law.[19]

Organization for Economic Cooperation and Development Guidelines:

The guidelines for the Security of Information Systems, 1992 have been formulated by OECD. The objective of security of information system is the protection of the interests of those relying information system from harm resulting from failures of availability, confidentiality and integrity and formulated some principles to be followed:[20]

Principles related to Information Security:

(a) Accountability Principle : The responsibility and accountability of owners, providers and users of information systems and other parties concerned with the security of information systems should be explicit.
(b) Timelines Principle: Public and private parties at both national and international levels should act in a timely coordinated manner to prevent and to respond to breaches of security of information systems.
(c) Democracy Principles: The Security of information systems should be compatible with the legitimate use and flow of data and information in a democratic society.

Adequate measures for security of information system help to ensure the smooth functioning of information systems.

Information Security and India:

In Nov 2012, India established the National Cyber Security coordinator as the overarching body for securing cyber systems, supported by four agencies i.e., The National Technical Research Organization, The National Critical Information and Infrastructure Protection Centre, The Computer Emergency Response Team, and the Ministry of Defence. India also has a cyber security coordinator in the National Security Council Secretariate.[21]

National Cyber Security Policy 2013:

The National Cyber Security Policy outlines the basic objectives and strategies to build a secure and resilient cyberspace for citizens, business and government. It also envisages building a workforce of 5 lakh professionals skilled in cyber security in five years.[22]

India has seen a massive surge in the number of cyber security incidents in the past 10 years. According to data from the Indian Computer Emergency Response Team, from 23 reported incidents in 2004, the number of incidents increased to 62,189 until May 2013. For Indian companies, there has been a 20% increase in average losses as a consequence of security breaches, while the average cost per incident has increased to $414 from $194, according to PWC report.

To protect data of Indian Internet Users, the National Security Council (NSC) has proposed a three pronged action plan. This includes asking all e-mail providers to set up local servers creating an Indian E-mail Service and making it mandatory for government officials to use the e-mail provided by the National Information Centre (NIC). The NSC wants all data related to communication between two users in India to remain within the country. [23]

India has started many good initiatives and formulated far reaching policies in the field of Cyber Security. However, their actual implementation is still missing and making all these efforts futile.

Although India has established National Critical Information Infrastructure Protection Centre, National Cyber Coordination Centre (NCCC) of India,[24] Tri Service Cyber Command for Armed Forces of India, Cyber Attacks Crime Management Plan of India etc. None of them are coordinating with each other and all of them are operating in different and distinct spheres.[25]

Conclusion:

India is one among the leading countries which uses information technology, networks and internet. Though the country is technically sound, the legal regulation on information technology and information security is weak. India has no codified cyber law dealing with the whole aspect of information technology. Further, there is no strong mechanism to deal with Information and Communication Technology.

The available mechanisms are without coordination and they are at chaos. They are simply policy implementation authorities without crystal clear policies.

As the information security is a matter of international jurisdiction, International Conventions with implementing authorities are essential.

Information Security is very much possible, but we have to wait for proper legal regulation at national as well as at international level.

References:

1. Sharma, Pankaj, E-Governance the New age Governance (2010), APH Publication, New Delhi. P-75.
2. E-Governance Act, 2002 (USA).
3. Sec.3541, E-Governance Act, 2002 (USA).
4. Secs. 29-A, 167, 172, 173, 175, 192, 204, 463, 464, 466, 468, 469, 470, 471, 474, 476, 477-A of Indian Penal Code, 1860.
5. Secs. 17, 22, 34, 39, 47, 59, 65, 73, 81-A, 85-A, 85(B), 90,131 of Indian Evidence Act, 1872.

6. Secs. 2, 2A of Bankers Books Evidence Act, 1891 and Reserve Bank of India Act, 1934.
7. Secs. 50, 51, 52, 53 and 56 of Electronic Communications and Transactions Act, 2002 (USA).
8. Sec. 65 of Information Technology Act, 2000.
9. Sec. 66 of Information Technology Act, 2000.
10. Sec. 73 of Information Technology Act, 2000.
11. (1972) 2 SCC 788.
12. Sec.74 of Information Technology Act, 2000
13. A/RES/53/70.
14. 69th Session, on Developments in the field of Information and Telecommunicationin the context of International Security. Held in Midrand, South Africa.
15. Held in Midrand, South Africa on 6 May 1996.
16. Held in Geneva from 10 to 12 Dec 2003 (First Phase) and in Tunis from 16 to 18 Nov 2005 (Second phase) Retrieved from www.un.org/disarmament/topics/informationsecurity on 14 Feb 2015.
17.www.thecre.com/fisma/?p=2173 retrieved on 14 Feb 2015.
18. General Assembly Resolution A/RES/64 on 21 Dec 2009.
19. Michael Whitman,HerbertMahord, Principles of Information Security, e-book https://books.google.co.in retrieved on 14 Feb 2015.
20.www.oecd.org/internet/ieconomy/oecdguidelinesforthesecurity retrieved on 14 Feb2015.
21. www.cryptome.org/2014/05/ru-international-infosee.htm retrieved on 14 Feb 2015.
22. www.deity.gov.in/sites/national-cyber-security-policy-2013-1 retrieved on 14-2-15.
23. http://ptlb.in/csrdci/?p=228 retrieved on 14 Feb 2015.
24. NCCC carry out real time assessment of cyber security threats and generate actionable reports/alerts for proactive action available at http://www.the hindu.com/news/national/india-getsready-torollact-cyber-snooking-gencyarticle 4798049.ece.
25. http://ptlb.in/csodci/?p=259 retrieved on 14 Feb 2015.