Citizen and E-Governance- Cyber Law and Related Issues

By Na.Vijayahankar Cyber Law Solutions Ltd Chennai
(Presented at the AMIC Seminar in Chennai on December 12, 2000)

E-Governance has two dimensions. The first is the application of Information Technology for the improvement of Administration. Second is application of Governance to the emerging Cyber Society.

Even though, the concept of E-Governance (EG) is, in principle applicable to all types of Governance including Corporate Governance, the present discussion is focussed on traditional responsibilities of a Politically elected body (Government) entrusted with the administration of a society (Citizens).

This system of Governance consists of the Ministry and the Parliamentary /State Legislative systems, down to the elected representatives of the Village Panchayat (in India). It also includes the implementation machinery consisting of the Officials and any other organisations involved in the delivery of collective state administered services to the Citizens.

The essence of EG is the Communication between the "Governing" and the "Governed" and the test of "Good Governance" is a "Harmoniously Living Society".

The system of EG is supported by five major pillars viz.;
Computers
Connectivity
Content
Consumer/s
Confidence Building

"Computers" in this context refers to all the hardware and software requirements of Governance.
"Connectivity" refers to all the information carrier systems, bandwidth etc.
"Content" refers to the information that is exchanged between the "Consumers" of the system.
"Consumers" refers to all the human and human substitute systems that access and use the "Content" in the EG system.
"Confidence Building " refers to such of those measures that helps the Citizens develop a confidence in the E-Governance and encourages them to take to the E-Transformation. It is in this context that "Law" has a part to play along with "Education".

The Concept of Cyber Society:

One of the key features in EG is to recognize that it includes an attempt to Govern the component of the society, which is accessible through the "Cyber System". It therefore covers the "Cyber Society" within the "General Society". At the same time E-Governance also attempts to regulate the Cyber Society itself because the person and property of a Citizen are controlled by the Government.
Most of the Conflicts and Issues in E-Governance arise because of the inability to accept the existence of two different societies with overlapping jurisdiction.

While one of the pre-requisites of a functional EG is to ensure a deep penetration of EG at least beyond a minimum acceptable critical level, at any point of time it has to deal with a mixed society which consists of

1. The "Cyber Society"
2. "Non Cyber Society"
3. Adhoc Users of the EG system who have not evolved into the "Cyber Society"

The "Cyber Society" consists of those who have adopted the "Cyber Usage" to a substantial extent. They have a culture of their own. They own Cyber property and participate in E-Commerce. This Cyber Society has its own "Boundaries" even though they are not bound by the boundaries of the geographical world. Such boundaries may be defined by various technology parameters. One example of such a boundary can be "Digital Identity". Similarly, A gaming zone that requires a minimum of 128 MB RAM can be considered bound by the minimum hardware barrier.

The members of the Cyber Society namely the Netizens have their "Rights" such as the "Right to Exist in Peace", "Right to Freedom of Speech", "Right to enter into legally enforceable Digital Contracts", "Right to own and maintain Cyber Properties", "Right to carry on Online Business or Professional Practice" etc. The State may have the right to "Taxation" provided it is providing any "Community Services" such as "Cyber Policing", "Cyber Judiciary", etc.

If the Government has to ensure "Harmonious living " in a society which may consist of disparate interacting elements, there is a need for some "Norms" acceptable to the society which will be complied with voluntarily by a majority of the members. It is in the exception of cases when a member of the society transgresses the "Norm" that we say that a "Crime" has been committed and invoke the "Police" and "Judiciary". Ideally, a commonly accepted set of "Norms" evolves into the "Law" for the society after they are codified into the statutory books. Thus, "Cyber Laws" have an important role in representing and defining the norms of the "Cyber Society" that the system of EG tries to administer. If the "Laws" closely match the aspirations of the society, they will be voluntarily complied with by the majority and even "No Governance" may be "Good Governance". If the "Laws" are arbitrary, they lead to "Exploitation of Loopholes", "Corruption", "Rebellion" and "Terrorism". Then even the "Best Governance" will be "Bad Governance" to a section of the society.

One of the practical challenges in EG is to ensure that the "Cyber Laws" not only satisfy the requirements of the "Cyber Society", but also are acceptable to the "Non Cyber Society" with which it interacts as well as the "Occasional members of the Cyber Society". In a country like India, where the Netizen population is only around 2 Million now (expected to reach 20 Million in the next two years), while the Citizen population is over 1 Billion, the need of managing the "Digital Divide" and its consequences are also important factors in EG. The Cyber Laws have to therefore manage these "Inter Society" issues to the Satisfaction of both the societies.

The Cyber Laws in the Indian Context came into focus with the Information
Technology Bill-1999, which has since been passed as Information Technology Act-2000 (ITA-2000). This was the first comprehensive codification of Laws in India directly enacted for the regulation of the Cyber world.

The ITA-2000 was a big step in the direction of introducing Cyber Laws for India. First of all, it provides a legal recognition for Electronic Documents and Digital Signatures as equivalent to the "Written" or "Typed" or "Printed" counterparts. (Subject to a few exceptions). It also sets the framework of procedure and standards for Digital Signatures. It also defines actions that are considered "Cyber Crimes" and suggests punitive measures. Besides, ITA -2000 has also defined the judicial system for trying and awarding punishments for Cyber Crimes.

In addition to the above, in the field of "Government-Citizen" (G2C) relationship management, the following three sections of the ITA-2000 directly address the requirements of G2C (Government to Citizen) relationship management.

**Sec 6: Use of Electronic Records and Digital Signatures in Government and its agencies :**

1. Where any law provides for
   the filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in particular manner;
   the issue or grant of any license, permit, sanction or approval by whatever name called in a particular manner;
   the receipt or payment of money in a particular manner, then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government.

2. The appropriate Government may, for the purposes of sub-section (1), by rules, prescribe -
   the manner and format in which such electronic records shall be filed, created or issued;
   the manner or method of payment of any fee or charges for filing, creation or issue any electronic record under clause (a).

**Sec :7 Retention of Electronic Records**

1. Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, -
   the information contained therein remains accessible so as to be usable for a subsequent reference;
   the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;
   the details which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the
electronic record: Provided that, this clause does not apply to any information, which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

(2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

Publication of rules, regulation, etc. in Electronic Gazette.

8 Publication of rules, regulation, etc, in Electronic Gazette:

Where any law provides that any rule, regulation, order, bye-law, notification or any other matter shall be published in the Official Gazette, then, such requirement shall be deemed to have been satisfied if such rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette:

Provided that, where any rule, regulation, order, bye-law, notification or any other matters published in the Official Gazette or Electronic Gazette, the date of publication shall be deemed to be the date of the Gazette which was first published in any form.

The above provisions provide a good framework for the Government departments to adopt E-Governance practices if they desire.

However, there are some noticeable shortcomings in the ITA-2000 a detailed discussion of which is beyond the scope of this note. In addition, several aspects of Cyber Laws are being additionally introduced through Telecom Regulatory guidelines, the proposed Communication Bill etc., The impact of these "Back door laws" needs to be assessed carefully for their impact on the Cyber Society.

The shortcomings observed so far in the regulations indicate that the Netizens need to closely monitor provisions, which may be misused during the EG process by various functionaries of the Government including the Police and the Regulatory Officers. There are several Ambiguities, Loopholes, besides Creation of New Power centers, Lack of Accountability, Over Regulation and Genuine Mistakes in the legislation. Any or all of them may lead to harassment of honest Netizens and continuance of inefficient and corrupt Governance.

The shortcomings observed so far in the regulations indicate that the Netizens need to closely monitor provisions, which may be misused during the EG process by various functionaries of the Government including the Police and the Regulatory Officers. There are several Ambiguities, Loopholes, besides Creation of New Power centers, Lack of Accountability, Over Regulation and Genuine Mistakes in the legislation. Any or all of them may lead to harassment of honest Netizens and continuance of inefficient and corrupt Governance.

We must consider ourselves to be fortunate that we are in a position to interact with the Legislators and record our comments when the “Constitutional provisions for the Governance of the E-Society”, in which all of us have a stake, are being formulated. Let's make full use of this opportunity, as otherwise, we will be abdicating our "Right to Good E-Governance".

(Proceedings of the seminars on "e-Governance & Democracy in the Millennium:
Challenges & Opportunities" held at Radha Park Inn International, Chennai on December 11-12, 2000 as a national conference of AMIC-INDIA.) Source: http://www.inomy.com/