

E-GOVERNMENT: A PROPOSED LEGAL & REGULATORY FRAMEWORK

Mohamed Y. Alem

Alem & Associates

Beirut – Lebanon

I. Introduction

E-government can be defined as the use of information and communication technologies (ICT) by a government for the conduction and support of its operations, for the provision and delivery of public services and for its engagement with citizens.

E-government facilitates the interconnection of relations between the government and its agencies, citizens and business entities.

Enhancement of the public administration's management and improvement of the delivery of public services are the primary results of e-government. E-government can also improve government efficiency, effectiveness, transparency, revenue growth, accountability and relationship with citizens, businesses and industries.

E-government assumes three basic forms of expression or phases:

a. Informative

Governments produce massive amounts of information and such information in the majority of cases is directed and/or useful to third parties (citizens, individuals, businesses, etc.). The use of ICT, especially the Internet, enables the easy and fast access to such information by such third parties, wherever they are located.

The publishing of government information online seeks the dissemination of public information to a wide audience; lessening geographical barriers, required time for such dissemination and optimizing transparency.

The content of government informative websites may vary from information related to the activities of such government, to public documents and records, laws and regulations, government knowledge, research, studies, administrative forms, etc. Indeed, such an informative phase constitutes the basic structure of e-government and with it a government establishes its “web presence”.

b. Interactive

An interactive e-government allows citizens to get involved in the governance process through enabling direct two-way communication (Government to Citizens) by means of e-mail (complaints, government processes, etc...), discussion forums, government networks, e-polling, etc.

In this respect, citizens may be able to be directly engaged in regulatory and policy processes, while having easier access to legislative projects’ information and are able to express their opinions, exchange ideas and interact with the government.

The use of such two-way electronic communication facilitates citizen’s participation in the public decision-making process, thus enhancing democracy.

c. Transactional

At a more advanced stage and complete e-government development, ICT is used to enable the government to perform complete transactions and to deliver services online.

Essentially, there are three types of e-government transactions: Government-to-Citizen (G2C), Government-to-Business (G2B), and Government-to-Government (G2G).

G2C transactions include the delivery of basic services to citizens such as issuance and renewal of civil status certificates, ID cards, and filing and payment of income taxes and fines, etc.

G2B transactions include various services exchanged between government and the business community, including application forms and renewal of licenses and permits, registering companies, obtaining permits, and payment of taxes and fines.

G2B transactions also include electronic procurement, which makes the bidding and tendering processes more transparent and efficient.

G2G transactions relate to all government interagency transactions (national and local governments and related agencies and offices), such as inter-government funds transfer, human resource management, etc.

At this point e-government assumes a more complex structure and a proper legal environment will be decisive as to the success or failure of the goals of e-government.

II. Key Issues for a Successful E-government

Implementing an e-government strategy is not simply providing governments with computers and automating the public administrative procedures. E-government is a complex subject and the success of e-government is measured by the achievement of its goals and objectives.

Several elements are directly and fundamentally responsible for assuring the establishment of a secure foundation to build upon the e-government structure. Such elements shall be carefully examined, considered and applied before the effective implementation of e-government.

The proper structure for e-government will require technical, administrative and regulatory reforms. Some of these fundamental elements can be identified as follows:

a. Strategy Development:

Each government having its own priorities, hence, e-government goals and objectives may vary from country to country. E-government shall be designed based on such individual priorities and aiming at the realization and achievement of its individual goals and objectives.

Due to its complexity, individual characteristics and the vast issues interrelated therewith, e-government is a process that requires strategic planning prior to its implementation. Such plan shall clarify, organize and strategize the forms by which

the government will use e-government to achieve its goals and objectives fulfilling national needs and expectations.

The prior development of a clear, complete and strategic plan is essential for the success of e-government projects. This strategic plan should determine all key areas to be addressed by e-government, its specific goals and objectives, policies necessary to support e-government, its methodology and implementation process.

In this respect, it is advisable for the government to establish a specific mandate for e-government and to create special committees and groups with the purpose of building such e-government plans and policies.

In structuring such e-government strategic plans and policies, it is recommended to allow the participation not only of related government agencies and bodies, but also of the private sector and civil society. Both, government and non-government stakeholders shall participate in defining the strategy and goals of e-government.

b. Infrastructure Development

A technological and human resource infrastructure shall be ready and compatible with the e-government features.

Due to the fact that the Internet strongly depends on the telecommunications system, a country's telecommunication infrastructure is one of the key factors for the successful implementation of e-government. This shall include the availability of telecommunication services, telecommunication service's rates, affordability and reliability of networks access.

In this respect, it has been demonstrated that telecommunications liberalization and private participation brings notable improvement to the telecommunication infrastructure.

Availability of telecommunication services, accessibility, affordability, proper and secure computer networks, modern system applications, etc. shall be carefully considered in order to better accommodate e-government activities.

The proper accomplishment of e-government depends not only on the technical, but also on human resources/capital. In this respect, the administration will need individuals to understand, create content and manage e-government initiatives.

Aside from public employees' special in-house training provided by the government, the basis of a country's educational system shall provide for ICT literacy, therefore creating a technological updated human resource.

c. Regulatory Reform

Government activities are strongly regulated and driven by legal frameworks including national constitutional laws and other related laws and regulations. Therefore, e-government shall be first supported by local laws and regulation for the sake of its legitimacy and legality.

Furthermore, when e-government moves from the passive provision of information to an interactive phase (whereby government services are being electronically delivered or the government is acquiring services and/or goods online) e-government assumes an equivalent form of e-commerce, having however the public administration acting in one of the poles of the transaction.

Therefore, and like when dealing with e-commerce, the parties involved in such transaction (government, individuals or businesses) are looking for basic assurances such as security, integrity, authenticity, confidentiality and data protection/privacy.

A successful e-government shall be sustained by an environment free of legal barriers and therefore, a legal reform shall be adopted to support rather than obstruct e-government.

Worldwide, we have witnessed two basic regulatory approaches for e-government: the Fragmentary and Specialized approaches. Several factors may drive a government to choose the type of regulatory approach it will follow, including the country's type of legal system.

The fragmentary regulation approach does not regulate e-government directly. It will have certain provisions within laws and regulations which will refer to e-government.

The fragmentary approach will treat issues related to e-government individually, thus covering the isolated legal aspects of e-government, such as digital signature laws, data protection, etc). In such cases, e-government regulation may face incoherence problems as such individual laws and regulations may not follow uniform principles and thus may miss the “global picture” of e-government.

The specialized regulation approach adopts specific uniform legislation covering fundamental legal principles, requirements and the management of e-government activities. Such approach usually assumes the form of a basic legal act specifically directed to the regulation of e-government, its development and processes.

A regulatory reform may be implemented, either by modification of existing laws and regulations (partial amendments), and/or by adding new provisions to existing laws (covering subjects currently not covered by existing laws), and/or by the enactment of new laws and regulations aiming at the creation of a favorable legal environment that would support e-government in all of its aspects.

Among international models regulating e-government, we encounter a broad list of subjects that are addressed by such laws and regulations such as e-contracts, terms of delivery and guarantees, provision of online services, data protection and privacy, security and reliability, electronic signatures and proof, electronic payments, consumer protection, intellectual property rights, cross border transactions, cyber crime, taxation, telecom sector, etc...

III. Basic Legal Infrastructure

Notwithstanding the regulatory approach chosen by a country to regulate e-government, it is certain that national legislations shall be first updated in order to legitimize the government to “electronically” operate and provide for services. Furthermore, such regulatory reform shall aim at the recognition and regulation of electronic documents and transactions, including issues related to security and privacy.

There is no one single model of e-government regulation. Most of the countries have recently started to enact laws and regulations in this respect. There are, however, certain essential legal subjects that shall be tackled by such regulatory framework and may be considered as common to most governments.

A proper legal infrastructure shall enable e-government to achieve its purposes without encountering legal barriers and impediments, and fundamentally shall focus on the following:

a. Legitimacy

As government activities are strongly regulated and driven by legal frameworks including national constitutional laws and other related laws and regulations, for legitimacy and legality purposes, a proper legal framework shall allow the government to conduct its administrative procedures, execute its functions and provide for services in electronic/digital forms.

b. Recognition of Electronic Documents and Transactions

Local laws and regulations shall create legal certainties for transactions conducted in an electronic format. Therefore, such laws and regulations must ensure recognition and functional equivalence between electronic and paper-based transactions, providing for a legal binding effect of such transactions and legal recognition of data messages, electronic signatures and electronic evidence.

c. Authentication

When electronic documents and transactions are legally recognized, and the government is authorized to provide services and conduct its administrative functions in an electronic form, other legal issues arise and therefore shall also be addressed by local laws and regulations.

Since many government documents have prescribed formats that require a handwriting signature, the recognition and regulation of electronic authentication shall be a key issue to be regulated.

The authentication methods shall vary according to the levels of assurance and security needed to validate such e-government related transaction. There are several electronic authentication methods being currently used by governments while conducting e-government transactions including the use of passwords, personal identification codes (PINs), user IDs, etc. Smart cards and biometrics technologies are also being assessed, however due to the high cost for their development we shall expect such authentication methods to be used in the future.

Some e-government transactions shall require security assurances other than authentication. Certain transactions will require the assurance of other fundamental aspects of information security such as **integrity** (the ability to determine if a message or other data has been altered since it was reduced to final form), **confidentiality** (the ability to prevent and detect unauthorized access and attempts to access a message or other data) and **non-repudiation** (the undeniable proof of participation by both the sender and receiver in a transaction). In such cases, international best practices have been adopting digital signatures and digital certificates (PKI) as an appropriate electronic authentication method.

Therefore, and notwithstanding the methods used for electronic authentication, it is intrinsically necessary that a legal reform validates and regulates electronic authentication and digital signature issues, including, but not limited to all issues related to third parties certification authority.

d. Data Privacy

Derived from the above mentioned authentication mechanisms and through everyday transactions, governments end up collecting an immense amount of data from individuals and businesses which are stored in the government's databases. In connection with several e-government related transactions, users may be asked to entrust to the government sensitive personal information such as financial, personal, medical, etc.

Privacy refers to the right for personal information attributed to an individual to be treated with an appropriate level of protection. Protecting the privacy of citizens and assuring them that their personal information will not be compromised is

fundamental in e-government and constitutes one of the keys to encourage the use of e-government.

Data Privacy related laws and regulations shall be enacted and enforced and shall apply to private and public sectors. Furthermore, government websites that collect private information from third parties shall adopt a data privacy policy establishing the principles by which such data is collected, stored, used, etc.

e. Freedom of Information

The public's right to reasonable access to government information is a cornerstone of public services. Such right to access public information "freedom of information" is fundamentally linked to e-government and shall be addressed by local laws and regulations.

Freedom of Information laws and regulations shall enable the government to achieve some of the purposes of e-government, such as more effective public participation in the governance processes as well as improvement of the government transparency.

f. Cybercrime

Another key subject to be addressed in the legal and regulatory reform that shall remove legal barriers for e-government, is the consideration and sanctioning of crimes committed under "cyber/electronic" environment.

The growing danger of crimes committed against computers and networks is alarming the whole world. In the majority of countries around the globe, existing criminal laws and regulations are likely to be unenforceable against such "cybercrimes".

Cybercrimes can assume a variety of faces: network sabotage, data interception, network intrusion, virus dissemination, data theft, unauthorized access, electronic fraud and electronic forgery, data alteration, etc.

Adequate legal protection and enforceability of laws and regulations against such crimes shall contribute in making the “cyberspace” an adequate and safe place for governments to conduct their administrative functions and to provide for services.

IV. Best Practices

Under international standards and best practices witnessed in the creation of a proper legal framework for enabling e-government, we can identify the following principles that should be considered by legislators while structuring such e-government regulatory framework:

- a. Consultation with stakeholders:** to better assess the existing laws and how they may obstruct the achievement of e-government’s desired results and objectives.
- b. Single Package of Directives:** specialized regulation is seen as the best approach for e-government however, and as seen above, adoption of specialized regulation may not always be possible due to several factors, including the differences of legal systems among countries. Despite the regulatory approach taken, it is incontestable that an integrated package of related laws and regulations on e-government shall enable more consistency and coherence on the subject matter, while related laws and regulations part of such package are to be drafted in accordance with uniform principles.
- c. Neutral Technical Approach:** when technical issues are addressed by laws and regulations, such as when tackling security and authentication, the legislator shall use simple technology and technology neutrality, removing related legal obstacles without tying up such issues with the use of a specific technology.
- d. Guidance for Implementation Process:** e-government and all legal aspects related thereto are somehow new to citizens and public servants and therefore, a proper and continuous guidance for the implementation of e-government regulation shall be made available including the draft of related regulatory implementation guidelines, policies, proper training and awareness of the public.