E-Governance: A New Reality for Legislative Drafting

Parisha Singh[1]

Abstract

The rapid development of modern information and communication technologies (ICT) over the past decades has led to changes in almost all areas of society. There are many ways in which governance can use ICT in order to become more efficient, user-friendly and transparent. E-governance has become a fashionable term, even if the definition of what it actually is can vary or be vague.[2]Some questions of governance can be quite different in the framework of e-governance while others remain the same, only in a new form. For legislators and thus for the drafters of legislation the question arises how a transition to more e-governance should be reflected in law. There will be a need for some new legislation but even more than that, it is essential for legislators and regulators to determine how to fit new phenomena into legal frameworks created for a different situation. Legal issues of e-governance do not form a single, unified area of law. It is important to note that e-governance does not necessitate a comprehensive system of specialised legislation. Actually, it might even be dangerous to have too many specialised laws because this runs the risk of creating a parallel system of governance. In such case, the efficiency gains that e-governance should lead to may be lost. In addition, too much regulation of technical matters may stifle innovation. Over-regulation can lock in technologies when instead flexibility is needed as technology moves so fast. Laws and other forms of regulations should address the nature of services and transactions or the type and sensitivity of data, in a technology-neutral manner.

[1] Student, 3rd year, GNLU, Gandhinagar.

[2] M. Sheinberg and T. Bartley,*Organizations, Regulation, and Economic Behaviour: Regulatory Dynamics and Forms from the Nineteenth to Twenty-First Century*,4 ANNUAL REVIEW OF LAW AND SOCIAL SCIENCE31, 38-39(2008).

Introduction

Much of the legal and legislative work related to e-governance consists of analysing existing legislation and through that identifying gaps or potential obstacles that necessitate legislative drafting. Questions of electronic identification and digital signatures is identified as one area where new rules are normally needed, because it is important to ensure that something as essential for the legal system as knowing the identity and being able to indicate will are clearly delimited in law. Furthermore, the way to give a signature electronically is quite different that in the non-virtual paper-based world. Something self-explanatory because known for centuries in the non-virtual world may need regulation in the virtual one. This is why a "signature creating device" can need regulation, while law does not normally explain what a pen with which one gives traditional signatures should look like. In addition, special focus should be put on data protection legislation because electronic data is generally perceived as less secure than traditional paper-based data. Even if such a perception is not necessarily true, it may cause people to be wary of e-transactions. It is not unusual that countries introduce various e-services only to find that people are not interested in using them - because of concern for data protection, because the services are seen to be complex or as there is a need for a special and complicated mechanism to get access to the services. This can lead to a vicious circle, if e-services are not used and as a consequence more such services are not developed - in turn further diminishing interest for them. Insufficient data protection legislation may also mean that loopholes of data security are abused. In data protection, as in many other areas, law and technology should work together, with technical solutions employed to protect data and law obliging such solutions. Today, Estonia is a world leader in e-governance.It is among the states with the most services offered and used on-line, significant use of digital signatures and several innovative uses of e-services, like on-line voting. Estonia has only very little legislation that is directly linked to e-governance.This is to ensure that benefits of e-governance can permeate the legal and administrative system of the country and e-services be integrated into general laws governing the various services. This article discusses how to make rules for e-governance. It looks at methods of law- and rule-making in high-technology areas. As e-governance is one type of use of cyberspace, the issue of how to regulate anything for this environment is of interest.

Regulating Cyberspace

Legislative questions of e-governance include general, even mundane, questions of administrative or procedural law and how to adapt these to the new technologies used. What however also is relevant is if and how the cyber environment can be regulated at all. Until relatively recently, many argued that the cyber world, with its borderless nature and its possibility for anyone to directly provide services, spread messages and do so with a globalreach, means that there should be no legal regulation at all of cyberspace. If this would be the case, it would affect e-governance just like any other services using the cyber environment. Perhaps e-governance is also one of the best examples why such thinking is not useful: cyber activities are not activities that are totally divorced from the non-cyber world, but they are actions taken in a new environment, which means that in many ways, similar rules should apply as for such various activities in whichever context. It is another question that it can be very difficult to regulate cyberspace because of its borderless and fluid nature.

When considering development of rules for cyberspace it is logical to look for analogies among other areas of regulation of rapid technical developments. Areas may show some common features when it comes to law-making, even if the issues are not alike, or on the contrary, highlight what needs to be different. Thus, we can compare cyberspace and outer space that have more than the name in common. These are international areas that do not pay attention to national borders. Technology is a key to the utilisation of the areas. There are however important differences in the approach of law for these topics. Outer space law developed at a time when space activities where almost exclusively public, while cyberspace use started with predominantly private activities. Outer space use (from the first satellite the Soviet sputnik, launched on 4 October 1957) just like cyberspace developed without there being a legal framework or any common understanding of what such a framework could be. However, quite soon rules emerged - helped by the public nature of activities, which meant that states could negotiate and agree in a diplomatic setting. Before there was any binding space law, basic legal principles for space were set out in the 1963 Space Declaration. The Declaration was in the form of a UN General Assembly resolution and as such not binding. Even so, it was of great importance as it was the first official document that stipulated principles of international space law. If state parties to an instrument accept its importance, its formal non-binding nature matters less. Such law-making is not effective for private parties, who need legal certainty and who do not have the possibility of the diplomatic give and take. For outer space, many of the principles of the Declaration were repeated in the 1967 Outer Space Treaty and gained legal abidingness in that way. As long as states are the main actors, also other elements of law-making can be identified. In this way, outer space law provides an interesting showcase for development of international law. From a non-binding and nevertheless important declaration to an international treaty, it is also likely that certain principles have become customary law.Customary law may despite its name develop quickly if the main parties agree on the relevant issues. The expression 'instant customary law' originates from outer space law.[3] The fact that the law dealt with something technically very new contributed to the understanding that such law can develop fast. The combined process of codification and progressive development through customary law can help deal with the need to accommodate technological change. However, when the main players are not states, the tools for development of law are different. In cyberspace, it would be difficultto identify the key players who could develop instant customary law - or more likely, the key players would be private enterprises and not states and private subjects are not seen as originators of customary law.

In cyberspace, private firms reached great importance before there were many rules at all. It is the difficulty of the traditional legislative system to keep pace with developments in cyberspace that has led to more innovative ideas about rule-making in the cyber context. To avoid over-regulation while still providing a sufficient legal basis, concepts such as multi-stakeholders and self-regulation attract interest. Self-regulation is regulation by subjects themselves or their peers, through a regulatory organ or in some loser fashion. The mandate to adopt rules and implement these derives from the participants in the system, which can be more or less formalised. In addition, such a system may cost less and help avoid disputes in the courts. Self-regulation in areas where there is rapid change, for example through the introduction of new technologies can more quickly and easily take into consideration all sorts of new factors that the legislator may struggle with, given the time usually involved in the regular legislative process. Internet developed so quickly that it has remained largely unregulated, as legislators and regulators were faced with a fait accompli that was difficult to intervene in once they had caught up with developments. As it is difficult and there is a lot of resistance to formal regulation of cyberspace, self-regulation could be appropriate, but whether that also means that sector participants are interested in it is another matter. The knowledge that no legal system likes legal voidmeans that sector participants are open to self-regulation, to anticipate a more heavy-handed approach. What this would mean more specifically is however very open.

Data: The Key Ingredient in the E-World

Moving "down to earth" from the higher reaches of cyberspace, we find that as concerns what this new environment can be used for, services in the digital world to a very large extent

[3] Bin Cheng, *United Nations Resolutions on Outer Space: "Instant" International Customary Law?*, 5 IJIL 23, 23-48(1965).

depend on data. Thus, data has become a valuable commodity. As a corollary, possible abuse of data is a real risk. Data protection is a human right, derived from the right to privacy. In Europe, the right is protected by the European Convention on Human Rights through its provisions on protection of privacy, Article 8, as well as by the Charter of Fundamental Rights of the European Union, which is the first international instrument to have an explicit data protection provision (Article 8) in addition to the general privacy protection (Article 7). By mentioning data protection specifically, the Charter of Fundamental Rights underlines the importance of it not least seen against an increased use of ICT.

In the relation to e-governance, data protection is important not least for the perception and trust of it. Governance and the public services offered through e-governance are largely not voluntary and if a state expects its subjects to provide data in the framework of various publicservices, it must also ensure that people have faith in the system. For e-governance, the state is under obligation to provide this feeling of comfort. Successful e-governance is built around interoperability of databases, meaning that data held in various databases can be used seamlessly by different authorities and for different contexts. This however could mean that any breaches of data protection could have widespread negative consequences. In Estonia, one important tool that also illustrates the necessary link between law and technology - is that any access to personal data by an authority leaves a footprint, so the person can see that his or her data was accessed, by which authority and when, by just logging in to the personal pages that every Estonian resident have in the e-governance system. This is the kind of measure that enhances the trust in the system. Protection of data is not the only possible legal issue. For data to be useful in interoperability context there are some other criteria that should be kept in mind. Standardisation at different levels is needed, to achieve semantic and technical interoperability. There is no need for identical formats but there must be rules on data representation formats and similar. Such rules may be rather technical in nature but evidently the legal system plays an important role, as there must be some basis for making application of the relevant standards compulsory for those that take part in the interoperability framework.

New Law or Old Law in A New Reality?

Areas of law that are affected by e-governance include among other administrative legislation, administrative and criminal procedural legislation, intellectual property law and consumer protection law. A key factor determining successful transition to e-governance is the establishment of a governing authority responsible for different aspects of e-governance.

The competence of this agency must be set out in law to avoid ambiguity and disputes. A well-functioning such body that can adopt the relevant rules as well as ensure their implementation may be what determines the success of e-governance. The question of approving a signature or other identification should not be related to the form but to whether it is capable of fulfilling its function of authenticating something. Relevant in this context is whether the signature is susceptible to intervention, modification or technical compromise.Digital identification systems are the entry point to e-services. Several concepts of digital signatures are in need of clarification while for traditional signatures some elements are self-evident.Although there are many possible ways of digital identification, for secure electronic signatures it is common that they consist of different keys - a private and a public one. This is linked to certification authorities that issue and control identification systems that ensure the validity of the signature. Here there is a clear role for the law and something that normally necessitates new legislation as the law needs to require such systems - often something new that either leads to the creation of a new authority or otherwise new tasks for some body. In addition, an important role of the law is to ensure acceptance of signatures.[4]These musthave the same force as regular signatures and such force shall be provided by law. Details of data exchange are stipulated in service level agreements between concerned parties (i.e. authorities having data and those needing access to it). Thus, the legal environment consists of specific and technical rules, based on a legal mandate given to stipulate sufficient criteria for a system of interoperability to function.

ICT Law, Cyber Security And E-Governance

It is so obvious that it is often forgotten in the debate that access to ICT is a prerequisite for e-governance. Thus, the legislation ensuring such access is essential. It is not e-governance legislation as such, but a necessary corollary. When a state transitions to more and more e-governance, the state has a responsibility for ensuring internet access of sufficient speed and quality to a reasonable price. Questions on providing real access are similar to the issue of the universal service obligation.[5] This found in the sector-specific legislation that complements general competition law.[6]Electronic communications law aims to create the necessary conditions for promoting the development of electronic communications networks and

[4] B. H. Malkawi, *E-Commerce in Light of International Trade Agreements: The WTO and the United States-Jordan Trade Agreement*, 15(2) INTERNATIONAL JOURNAL OF LAW AND INFORMATION TECHNOLOGY153, 163(2007).

[5] Case C-320/91 Corbie and Case C-280/00 Altmark, European Court of Justice.

[6] L. De Muter, *Regulatory Asymmetry? The Competition Between Telecommunication Operators and Other ICT Players*, 3 JOURNAL OF EUROPEAN COMPETITION LAW & PRACTICE 452, 453-54 (2012).

services while ensuring the protection of the interests of users of such services. Legislation normally provides rules for how to enter the market, whether a licence or general authorisation is needed and in that case how it is obtained; what rules there are for service provision; and how monitoring and supervision are conducted. Apart from setting the conditions for normal operation of ICT, the legislation has to deal with cyber threats as well. These have to be tackled in many contexts and one special feature of the cyber world is that private companies are so important that they will normally be the main responsible for security matters as well. At the same time, cyber security is an essential component of defence policy (and law) as well as criminal law and law enforcement. The National Cyber Security Index (NCSI) is a useful tool to see what the different components of cyber security are. Often this notion is seen as either linked to military security or to crime, not seeing how cyber security really needs a total look at very many components. NCSI is still under development as far as the ranking of different countries is concerned, as this is a time-consuming activity, given that all statements have to be based on available evidence. However, the indicators can provide a very useful checklist for those drafting legislation and other instruments on cyber security. A number of issues such as a secure environment for e-services, e-signatures and identities, are included. Development of e-governance can thus move hand in hand with development of a more secure cyberspace.

Conclusion

E-governance appears as something new and highly technological, a complex collection of technical requirements for how to prove identity, how to protect infrastructure, how to share data and interact with different parties. It is quite common that when states prepare for e-governance, they first of all do not involve lawyers until later in the period, as the matter is seen as an IT issue. Secondly, once the lawyers do get involved they start by drafting specific rules that in their complexity and comprehensiveness should match the complexity of the technology. This author is not trying to claim that e-governance or generally, cyber activities, are not complex. However, instead of focusing on the complexity and on what it is that is different, those involved - including those who deal with legislative drafting - should first of all take a step back and see what it actually is that is different just because the environment in which it happens is different.

For the protection of data for example, the essential issue is what the content of the data is: is it of sensitive nature or not. Although ICT has meant there are many more ways in which data can be used and also in which combinations of data or IT processing of it can generate knowledge that may be sensitive and that manual use of the same data may not have shown, despite this, in most cases the sensitivity of data is actually much less dependent on its form (electronic or not) than its content. Legislation needs to focus on risks and identify what measures that are needed to deal with these risks and not try to make rules on everything just because it is new and different.As the cyber world means that the physical presence is not a factor and signatures cannot be given in the way in which they have been for generations, legislation needs to deal with this new reality and explain what it is that replaces the traditional tools. Data in electronic format can be shared and used in new ways, which is what actually enables many e-services, but to be able to use this beneficially, systems need to be in place and these need a legal framework. Interoperability is only possible if the data systems can communicate - law needs to make sure they speak the same language.

So, in some ways, legislators and legal drafting professionals faced with e-governance are indeed faced with many issues to consider and new and complex questions. In other ways, the issue is not at all as complicated as it may appear at first glance. However, the fact cannot be escaped that the very way in which rules are made is in a process of change. The official legislators may find that their role is to some extent taken over by self-regulatory organs and multi- stakeholder where sector participants themselves feel that they are the best placed to decide the relevant rules. It is a challenging environment, requiring expertise and efforts of cooperation on all sides, but it is also one that may lead to better and more appropriate regulation - an improvement of governance and not just a new way to do it.