Chapter 6

Legal Regulation of Cyberspace

6.1 Introduction

Advances in the development and use of information technology and the electronic media for easy and extensive worldwide interaction is creating many legal issues and disputes both in relation to existing relationships as well as new forms of affiliations that require redefinition and new terms of interactions, respectively. The cyber world is amorphous with multiple parties interacting from different geographical and jurisdictional points. The development of the Internet infrastructure through the means of efficient categorization and organization of information and the methods for accessing and navigating the World Wide Web (www) poses challenges that require laws and regulations in order to provide legitimacy to their existence and to create an orderly and effectively functioning transactional framework, wherein all its participants are aware of their rights and responsibilities vis-a-vis one another. Hence, there is a growing interest in the identification of potential solutions to the uncertainties that arise from online relationships and networks.\(^1\)

Legal measures for regulation of cyberspace are system of rules and institutions that underpin cyberspace, facilitate orderly interaction and resolve disputes or conflicts that arise in spite of such rules. It also allows people in a community, to determine the limits of what can and cannot be done in their collective interest.\(^2\)

---


\(^2\) Ibid, at 6.
6.2 Cyber Law

Law governing cyberspace is defined as Cyber Law. It encompasses the rules of conduct:

1. that have been approved by the government;
2. which are in force over a certain territory and
3. which must be obeyed by all persons on that territory.

Violation of these rules could lead to government action as imprisonment or fine or an order to pay compensation. In cyberspace as in real space, law often follows change. Cyber Law can be created in many different ways; it can be negotiated, imposed or evolved. The speed at which information technology has developed requires a faster, more reactive and automatic response from the law that is not currently met by the existing law-making framework. There is need to seek inspiration from recognized sources of law from both domestic and the international legal systems to identify and give recognition to potentially new ones\(^3\).

6.3 Custom as source of Cyber Law

“Laws are Sand, Customs are Rock.”

The Gorky Incident, Mark Twain (1835–1910)\(^4\).

Customs in cyberspace are “informal social standards of obligatory user behavior in cyberspace practices that have developed through mutual user assent and in deference to the preferences of other users, rather than mere tendencies of user behavior. Cyberspace custom and common usage can form a regime of

\(^3\)Ibid, at 4.
\(^4\)Ibid, at 3.
rules that constitute the new cyberspace customary law and can be progressively developed and codified.\(^5\)

The development of rules to order and regulate intercourse in the digital world is slower than the pace and development of new forms of communications technology, electronic analogues and legal entities. Custom can provide an additional source of law and the impetus for national and international legislators as well as organizations to develop written norms, further clarify and substantiate such norms, and reinforce their acceptance and application. There are two main benefits to identifying the customary rules for cyber law. It will both give legal legitimacy to recognized, existing and established practices as well as speedily detect legal norms for newly emerging practices. ‘Customary International Law’ is meant to supplement existing and applicable laws, both international and country-specific, for any form of transaction, transnational or otherwise, and in every area of law and activity, not just for commercial transactions or in the area of e-commerce and contract law. It will act as a gap-filler of rules for new practices and technologies and as an interpretative aid for written law. It is complementary and is not meant to supplant explicitly written rules of policy and law, unless and to the extent that it supersedes them in a manner and according to a procedure that is clear and acceptable based upon a hierarchy of norms in the event of a conflict of norms.\(^6\)

**Legal Regulation of cyberspace by good governance**

Concept of “multi-stakeholder in governance” should be perceived as the new way forward in favor of the inclusion of the whole of society for regulation of cyberspace. Rules which serve as a benchmark for public participation, access to information and transparency in cyberspace governance as well as the

---

\(^5\)Ibid, at 18.
\(^6\)Ibid, at 5.
building of a common understanding of the respective principles and their practice, help to design a democratic environment in cyberspace. Legal regulation by good governance calls for procedures that establish equal bargaining powers and fair proceedings, as well as enhanced transparency and review mechanisms, which enable the allocation of accountability. Transparent minimum quality standards enhance the cyberspace conditions and the assessment of performance and accountability, as well as facilitate the coordination of governance related regulations. Transparent procedures allow for a certain level of “democratic” legitimization and predictability through active involvement of citizens as well as through certain control over the decision-making processes.

6.4 Regulation of Cyberspace by Legislature

Law can regulate behavior and that was in fact the challenge posed to law-makers by the increasingly busy and high volume of electronic activity in the cyberspace. The cyberspace can be regulated by developing an adequate legal framework after taking the underlying technology into account. The legal framework for regulation of cyberspace must include:

- Right-to-know-legislation;
- Prohibition-legislation;
- IT-security-legislation;
- Utilization-legislation;
- Task-force-legislation.


Ibid, at 29.
i) The **right-to-know-legislation** has the purpose to keep the neitizens informed about the applied legal scenarios. In the United States, several attempts have been taken to realize such kind of legislation\(^9\).

(ii) The **prohibition-legislation** introduces provisions, which envisage to forbid or at least to restrict the use in cyberspace. Such an approach is traditional in state legislation if the public community dislikes a certain behavior; enforcement of prohibition is possible (at least in the books). Self-regulatory mechanisms rather tend to introduce incentives (if at all) instead of prohibition\(^10\).

(iii) **IT-security-legislation** encompasses initiatives that demand the establishment of certain IT-security standards which should protect that application of cyberspace from unauthorized reading and rewriting. Such kind of provisions can be introduced by the state legislator, but also by self-regulatory mechanisms; typically, industry standards are developed by the concerned market participants, having therefore the chance to be observed by the respective developers\(^11\).

(iv) **Utilization-legislation** intends to support the use of cyberspace in certain scenarios. Therefore, the legislative approach has to fine-tune an appropriate balance between prohibited and utilizable approaches\(^12\).

(v) **The task-force-legislation covers** legal provisions supporting the technical community to invest into the research of the legal challenges of cyberspace; the purpose of this approach consists in a better understanding of the relevant problems\(^13\).

---

\(^9\)Ibid.
\(^10\)Ibid.
\(^11\)Ibid.
\(^12\)Ibid.
\(^13\)Ibid.
6.5 Jurisdictional approaches for Legal Regulation

Whereas traditional jurisdictional issues are geographically based, today electronic communication readily crosses borders without having any specific links to the territory where the technology is located and users engage in global activities without the need for physical presence within the forum state. As the cyberspace has become part of daily life rather than a place deserving an occasional visit, the courts of different countries strive to adapt existing legal systems to ever nebulous out-of-state cyber defendants. There are three possible jurisdictional approaches for legal regulation of cyberspace: the spider web approach, the highway approach and the cyberspace approach.

a) Spider Web approach

If the court adopts the so-called spider Web approach it assumes that “each person who places his message on the Internet places his presence at every point on the Web”. Adopting this approach, every state has concurrent jurisdiction over the Internet presence of a non-resident defendant based on the fact that a defendant who puts up a Web site should know that the site can be reached by anyone anywhere.

b) Highway approach

Internet is like a highway that people use to travel from one place to another or from one Web site to another. The courts have usually found that the fact that the seller has put up a Web site is not sufficient to establish personal jurisdiction and that browsing by the buyer is a necessary additional element to establish personal.

---

16 Ibid.
17 Ibid, at 151.
c) **Cyberspace approach**

According to this approach contracts over the Internet are unique and cannot be compared with traditional contracts governed by traditional personal jurisdiction rules, so they must be regulated by a separate set of rules, preferably under federal jurisdiction\(^\text{18}\).

Jurisdiction issue has been settled on the basis of Two European conventions\(^\text{19}\–\)

A) the *Brussels, according to this convention* defendant regardless of his or her nationality, must be sued in the contracting state of his or her domicile (Convention, 1968, Article 2) and

B) the *Lugano conventions* defines cases of special jurisdiction, with Article 5 permitting the following situations in which the defendant can be sued in the courts of another contracting state

- In matters relating to a contract the defendant can be sued in the contracting state of the place of performance of the obligation in question (Convention, 1968, Article 5(1));

- In the matters of tort, delict or quasi-delict the defendant can be sued in the contracting state where the harmful event occurred (Convention, 1968, Article 6(1))\(^\text{20}\).

The issue of development of legislature for regulation of cyberspace is global. Although some states are a bit slower than others, many have managed to pass statutes regulating some aspect of the cyberspace. Many others are caught up in the endless preparatory work of various committees appointed to deal with the problem. Through international organizations, such as ITU,

---

\(^{18}\)Ibid, at 152.

\(^{19}\)Ibid.

\(^{20}\)Ibid.
Chapter 6

Legal Regulation of Cyberspace

INTERPOL, United Nations Office on Drugs and Crime (UNODC), G 8 Group of States, Council of Europe, Organization of American States (OAS), Asia Pacific Economic Cooperation (APEC), The Organization for Economic Cooperation and Development (OECD), The Commonwealth, European Union, efforts have been taken to ensure the harmonization of legislation in the individual countries.\(^{21}\)

First legal order

The first legal order is based on geographically-defined and confined legal rules and system. The logic of territorially defined law is based on several considerations including national sovereignty, consisting of notions of “legitimacy” and “power”; and relevance and efficacy, due to the place of “nationality”, the “effects doctrine” and the reality of enforcement.\(^{22}\)

Second legal order

A second legal order developed consisting of rules for transactions that involved different parties and action over several territories. This falls under the umbrella of Private International Law that addresses private relationships and transactions, and the Public International Law framework that largely covers the relationship between nations and international organizations.\(^{23}\)

6.6 Legal Regulation of Cyberspace: Australia

There are literally hundreds of laws spread throughout the jurisdictions of Australia, which could potentially apply to criminal activity that targets the cyberspace, computers and information networks. The New South Wales


\(^{23}\)Ibid, at 10.
legislation in force prior to 2001 amendments contained general computer crime provisions that could also be used to over internet crimes. In June 2001 an amendment to the Crimes Act 1900 was enacted through Crimes Amendment (Computer Offences) Act 2001. This amendment Act was designed to tighten penalties for prohibited acts relating to computers and to introduce specific provisions covering viruses and hacking. Later the Cyber Crime Act 2001 was passed by Parliament on 27 September 2001 and given royal assent on 1 October 2001 to amend law relating to computer offences and other purposes. The Act inserted a number of new offences into Criminal Code Act 1995 and repealed existing computer offences provisions from the existing Federal Criminal Legislation. It also amends existing Federal Legislation including the Crimes Act 1914 and the Customs Act 1901.

The Critical Infrastructure Protection (CIP) strategy, which sources from the Trusted Information Sharing Network for Critical Infrastructure Protection (TISNCIP) was launched in April 2003 to protect the infrastructures of public and private sectors from computerized threats. The Cyber crime Act 2001 was passed to replace out dated law of offences.

**Australian Broadcasting Authority**

The Australian Broadcasting Authority (ABA) is the Australian Government regulatory agency with responsibility for administering a co-regulatory scheme for Internet content matters. In relation to Internet content, the ABA:

- administers a hotline for complaints about illegal and offensive Internet content

---

Net Alert Limited

Net Alert Limited is Australia’s Internet safety advisory body, established in 1999 by the Australian Government to provide independent advice and education on Internet safety and managing access to online content. Net Alert: It develops programs and resources to educate the community about Internet safety operates a toll-free national help line, providing free Internet safety advice and resources for the community. The help line has a particular focus on methods (including filtering) of managing Internet usage, particularly for children and their families, and has been designated by the Minister for Communications, Information Technology and the Arts as the body with which the Internet industry must consult when developing codes of practice.

6.7 Legal Regulation of Cyberspace: Austria

The Austria has passed a comprehensive legislation in the field of protection of privacy in cyberspace in form of Protection of personal data (Privacy Act) 2000.
6.8 Legal Regulation of Cyberspace: Asian Pacific Economic Cooperation (APEC)

In a joint statement at the Ministerial Meeting in Santiago, Chile, November 17-18, 2004, APEC leaders agreed to strengthen the respective economies ability to combat cyber crime by enacting domestic legislation consistent with the provisions of international legal instruments, including the Convention on Cybercrime (2001), and relevant United Nations General Assembly Resolutions.29

6.9 Legal Regulation of Cyberspace: Association of Southeast Asian Nations (ASEAN)

ASEAN has established high level Ministerial Meeting on Transnational Crime. At the Meeting in Bangkok, January 8, 2004, a statement recognized cyber crime and the need for an effective legal cooperation to enhance the fight against this transnational crime.30

6.10 Legal Regulation of Cyberspace: Belgium

The Belgium parliament has inserted new articles in Criminal Code in Nov. 2000 to combat cyber crime and made computer-forgery, fraud, hacking and sabotage punishable offences.31

6.11 Legal Regulation of Cyberspace: Brazil

The regulation of the governance of the cyberspace in Brazil dates back to 1995, when the Ministry of Communications and the Ministry of Science and

30 Ibid.
31 Ibid.
Technology issued a “Joint Note” about the Net. Federal Law has been interpreted to define the Internet as a private environment. Therefore, in Brazil, the Internet is not within the same legal public law-based framework as ordinary telecommunications are. It made it clear that the legal framework for the Internet in Brazil would be a private economic activity to be explored by private players, without the need for licenses from the Federal Government. Law can create legal dogmas to impose legal fictions in some relationships. Once those legal fictions are created by the law, and accepted by the society, they are also able to regulate any given situation. Legal dogmas often ignore the “architecture” of the real world. Legal dogmas can redefine the nature the way the law wants. Legal dogma is a legal statement that is accepted as true, for the juridical system, regardless of any scientific (or architectural) accuracy. The reasons why the legal dogma is accepted as true are many and they are related to the cultural aspects of each society and of each country.

6.12 Legal Regulation of Cyberspace: Bangladesh

The ICT Policy 2002 aimed at ‘building an ICT-driven nation comprising of knowledge based society by the year 2006’ The model suggested the four critical phases of e-government evolution, viz., the web presence, interactions, transactions and transformation.

6.13 Legal Regulation of Cyberspace: China

The main regulation for governing the network infrastructure and international network connections is the Temporary Regulation for the Management of Computer Information Network International Connection

\footnote{Available at egov.ufsc.br/portal/sites/default/files/anexos/5930-5922-1-PB.pdf.}

\footnote{Ibid.}

(Temporary Regulation). This regulation was formally announced on 1 February 1996 and verified on 20 May 1997\textsuperscript{35}. Article 6 of the Temporary Regulation provides that “all direct international networking traffic must use international incoming and outgoing channels provided by the national public network of the MPT.” This means that every bit of traffic that comes from foreign servers must pass through the network of the former MPT (now MII), making it easier to monitor the traffic. Subsequently Computer Information network and Internet, protection and management regulations were approved by state Council on December 1997 and promulgated by the Ministry of Public Security on 30 December 1997\textsuperscript{36}. These regulations were established on the basis of the “PRC Computer Information Network Protection Regulations” and the PRC Temporary Regulations on Computer Information Networks and the Internet and other administrative regulations in order to strengthen the security an protection of computer information networks and of the internet and to preserve the social order and social stability. Public Republic of China has also passed legislation known as PRC Electronic Signature Law to further boost its online business which became effective on 1 April 2005\textsuperscript{37}. By legalizing electronic contracts involving public utilities the act regulates not only China’s booming e-commerce industry but also its e-governance related market.

\subsection*{6.14 Legal Regulation of Cyberspace: Commonwealth}

In an effort to harmonize computer related criminal law in the Commonwealth\textsuperscript{58} countries, experts gathered together and presented a model law to the conference of ministers in 2002. That law, titled the Computer and

\begin{itemize}
  \item S.V.Jogarao, Law of Cyber Crimes & Information Technology Law, 310 (2007).
\end{itemize}
Chapter 6  Legal Regulation of Cyberspace

Computer Related Crimes Act, shares the same framework as the Convention on Cyber crime to limit conflicting guidance. The model law serves as an example of common principles each country can use to adapt framework legislation compatible with other Commonwealth countries.38

6.15 Legal Regulation of Cyberspace: Danish

The Danish Government IT security council established in 1995 by the Danish Minister of Research and Information Technology has adopted recommendations to public authority and private companies on how to carry out the transition to digital document management and still achieve the necessary legal security39.

6.16 Legal Regulation of Cyberspace: Europe

Council of Europe

The first international initiative on computer crime in Europe was the Council of Europe Conference on Criminological Aspects of Economic Crime in Strasbourg in 1976. Several categories of computer crime were introduced. In 1981 the Council of Europe (CoE) adopted a Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data40.

The Council of Europe Recommendations of 1989

The Council of Europe appointed in 1985 another expert committees in order to discuss the legal issues of computer–related crime. A summary of the guidelines for national legislatures with liability for intentional acts only, was

38Available at egov.ufsc.br/portal/sites/default/files/anexos/5930-5922-1-PB.pdf
in the field of Regulation of cyberspace by framing in 1995, the Data Protection
Directive\textsuperscript{41}.

\textit{Common framework for electronic signatures}

After elaboration of the text by the Working Group on 
Telecommunications of the Council and the Committee of Permanent 
Representatives a final proposal for Common framework for electronic 
signatures was submitted to the Council of Ministers for political agreement 
during its meeting held in Brussels on 27 November 1998. A political agreement 
could, however, not be reached on the directive and the Permanent Committee 
was instructed to further discuss the file. The most important reason for not 
agreeing on the proposal was the lack of consensus between the Member States 
on the need for requirements regarding the quality of the products used to create 
an electronic signature with full legal effect\textsuperscript{42}.

\textit{Directive 1999/93/EC}

Parliament and of the Council on a Community framework for electronic 
signatures was enacted after substantial deliberations both on the EU level as 
well as within the member states, the EU Directive on Electronic Signatures was 
adopted. The Directive comprises twenty-eight recitals, 15 articles and four 
appendices. The Directive’s aim was to, “facilitate the use of electronic 
signatures and to contribute to their legal recognition”\textsuperscript{43}.

\textsuperscript{41}S. Schjolberg, “The History of Global Harmonization on Cybercrime Legislation - The 
\textsuperscript{42}J.Dumortier and P.V.Eecke, “The European Draft Directive on a Common Framework 
\textsuperscript{43}A.Torrubia, F.J.Mora and L.Marti, “Cryptography Regulations for E-commerce and 
The Council of Europe has developed a Convention on Cyber crime. The Council of Europe Convention on Cyber crime was opened for signatures at a Conference in Budapest, Hungary, on November 23, 2001. This Convention is a historic milestone in the combat against cyber crime, and entered into force on July 1, 2004. The convention is really three conventions in one, covering three different sets of issues. The three sets of issues covered by the Convention are:

- Substantive computer crimes
- Government access to communications and computer data
- Trans-border cooperation.

Convention requires signatory states to criminalize a host of activities that, in one way or another, are connected to a computer, computer material, computer operation or computer system.

Offences are categorized into four groups:

- Group 1 - Offences against confidentiality, integrity and availability of computer data and systems.
- Group 2 - Computer-related offences.
- Group 3 - Content-related offences.
- Group 4 - Copyright-related offences.

---

Chapter 6

Legal Regulation of Cyberspace

The Convention aims to harmonize domestic laws setting out cyber crime offences;

**Sanctions**

Signatories to the convention are required to adopt a penalty scheme that is “effective, proportionate and dissuasive” and includes custodial sentences. The convention did not seek to set any level of sanction – something which has been perceived as a weakness.

**Corporate liability**

Another noteworthy aspect of the convention is that it requires signatory States to provide for corporate liability for commission of the offences established in accordance with the convention.

**Other new offences**

The Convention created a number of new offences which are not yet dealt with by any EU initiative. These include:

- Offences of using electronic means to commit forgery or fraud.
- Offences relating to distribution and possession of child pornography in a computer system
- Offences of infringement of copyright and related rights where the infringement is committed intentionally on a commercial scale by means of a computer system.

Issues include concerns about unnecessary interference with privacy and human rights and the costs to Internet service providers of collecting and

[48] Ibid, at 87.

182
maintaining information. These issues, together with the requirement to permit international access to information by governmental authorities in other jurisdictions make the conventions requirements very ambitious indeed.\textsuperscript{49}

Based on the Convention and the recommendations from regional organizations may prove to be useful in future to reach our goal of a global legal framework against cyber crime. The Commission of the European Communities presented on April 19, 2002 a proposal for a Council Framework Decision on attacks against information systems. The Council of the European Union adopted the proposal in 2003 and it entered into force in 2005.\textsuperscript{50}

With respect to the Convention, the Framework Decision (FD) on Attacks against Information Systems 2005/222/JHA\textsuperscript{2} places emphasis rather on approximation of criminal law improving cooperation between judicial and other authorities, calling for the use of existing networks of operational points. The FD on combat Child Pornography on Internet 2004/68/JHA\textsuperscript{3} calls Member States to promote and facilitate investigation and prosecutions, to cooperate with Europol and Interpol and also to build up dialogues with the industry. The Directive on Electronic Commerce 2000/31/EC\textsuperscript{4} is important in relation to issues of responsibility as it excludes same obligations of network operators to monitor the information they transmit or store. The Directive on Privacy and Electronic Communication 2002/58/EC\textsuperscript{5} besides containing provision on spam, envisages also an obligation for service providers to take measures to safeguard security and to inform users in case of a particular risk or breach of security of the network. The Directive on the Retention of Data 2006/24/EC\textsuperscript{6} is particularly relevant for the purpose of prevention, investigation, detection and prosecution of criminal offences as it ensures at EU level that certain data, in the


course of the supply of communications services, are retained for a certain period of time\textsuperscript{51}.

In latest development, the EU Commission considered an initiative in May 2007 with regard to European legislation against identity theft, called “Towards a general policy on the fight against cyber crime”. A Framework Decision amending the Framework Decision 2002/475 JHA on combating Terrorism has been prepared in 2008 in the European Union. The Recommendation of May 12, 2009, of the European Commission is a framework approach to legislate in the field of Internet security. The Recommendation provides guidance to Member States which then have to enact specific rules. While the Recommendation makes reference to EU Data Protection Directives, it does not stipulate any specific provisions itself. Therefore, a framework of substantive key principles set by a legislator at the international level, complemented by the private sector with more detailed regulation seems to be the best solution. Through such a framework, general pillars of regulation could be set for everyone, which are then suitable to be supplemented by the individuals concerned in a way that suits their current needs. Furthermore, the inclusion of an international legislator in the process also ensures the continued involvement of the public sector, contributing at least by monitoring the process\textsuperscript{52}.

6.17 Legal Regulation of Cyberspace: G-8 Group of States

The High Tech Subgroup of the G-8’s Senior Experts on Transnational Organized Crime developed and established in 1998 a 24-hour, seven day

network of experts to assist in high-tech crime investigation. At a meeting in Washington D.C. in 1997, the G8 countries adopted Ten Principles in the combat against computer crime. The goal was to ensure that no criminal receives “safe havens” anywhere in the world and that the law enforcement authorities have the technical ability and legal process to find criminals who abuse technologies and bring them to justice. Other countries have joined the network and are participating in the co-operation. The G-8 Group has also agreed upon principles that should apply when law enforcement agents employed by law enforcement agencies are investigating criminal offenses and require assistance in other countries. Such principles should be implemented through treaties and through national laws and policies.\(^5^3\)

### 6.18 Legal Regulation of Cyberspace: India

Information Technology Act, 2000 was passed to give effect to Resolution of General Assembly of United Nations dated 30 January 1997 where Model Law on Electronic was adopted. The Act provide legal Recognition to transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred as “electronic commerce” which involve the use of alternative to paper based method of communication and storage of information; to facilitate electronic filing of documents with the government agencies and further to amend Indian Penal Code, the Indian Evidence Act, 1872, the Banker’s Books Evidence Act 1891 and the Reserve Bank of India Act 1934 and for matters connected therewith or incidental thereto. In additional Information Technology (Certifying Authorities) Rules, 2000 were passed by Central Govt. for regulating the application and

\(^{53}\)Available at [www.usdoj.gov/ag/events/g82004/index.html](http://www.usdoj.gov/ag/events/g82004/index.html).
other guidelines for certifying authorities. In exercise of powers conferred by section 87 of Information Technology Act, 2000 the Central Government has also passed Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000. In December 2008, the Indian government hurriedly passed through Parliament a bill to amend India’s Information Technology Act (the “Act”). The amendments bring about far reaching changes, including the provision of some level of data protection in India for the first time, criminalizing various kinds of offensive conduct on the internet, punishing cyber terrorism and widening the defenses of intermediaries to cover mere conduit.

6.19 Legal Regulation of Cyberspace: Japan

The Information Security Policy Council in the Strategic Headquarters was then created in May 2005 in order to promote the advancement of secure information and telecommunication. The national security strategy, named as Secure Japan 2006 and decided by ISPC (Information Security Policy Council, 2006a), listed the priority measures and directions for 2006 and beyond.

6.20 Legal Regulation of Cyberspace: Malaysia

To control crime in cyberspace Malaysia has Computer Crimes Act 1997, which provides that the territorial scope of the Act: “shall, in relation to any person, whatever his nationality or citizenship, have effect outside as well as within Malaysia, and where an offence under this Act is committed by any person in an place outside Malaysia, he may be dealt with in respect of such

---

offence as if it was committed at any place within. The Act promotes e-commerce and e-contracts in Malaysia by legalising the use of digital signature technology.

6.21 Legal Regulation of Cyberspace: Malta

In Malta Electronic Commerce Act 2001 was enacted by and with the advice and consent of House of representatives in relation to electronic commerce and to provide for matters therewith or ancillary thereto.

6.22 Legal Regulation of Cyberspace: Mauritius

The Economic Crime and Anti money Laundering Act of 2000 was enacted by the Parliament of Mauritius to provide for the establishment of an economic crime office and for the prevention and punishment of money laundering and economic offences.

6.23 Legal Regulation of Cyberspace: Organization for Economic Co-operation and Development

In 1980 the Organization for Economic Cooperation and Development (OECD) adopted Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. In 1982 the OECD in Paris decided on appointing an expert committee to discuss computer-related crime and the need for changes in the Penal Codes. With respect to the transnational aspects of computer-related criminal activity, important issues were noted which point to the desirability for

---

60 Ibid, at 588.
International cooperation in repressing and controlling such activity. In 2002 OECD adopted new guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. The 18 member countries decided to obey the 2002 OECD Guidelines for the Security of Information Systems and Networks: Building up the Computer Emergency Response Teams (CERT), developing partnerships among participants, sharing best practices and adopting international standards are the results of OECD project\(^6\).

### 6.24 Legal Regulation of Cyberspace: Philippines

Electronic Commerce Act of 2000 was enacted by the senate and house of Representatives of the Republic of Philippines providing for the recognition and use of electronic commercial and non commercial transactions and documents, penalties for unlawful use thereof and for other purposes\(^6\).

### 6.25 Legal Regulation of Cyberspace: Romania

Title III of Anticorruption Law on Preventing and fighting Cyber crime regulates cyber crime by specific measures to prevent, discover and sanction the infringements through the computer systems, providing the observance of the human rights and the protection of personal data in Romania\(^6\).

### 6.26 Legal Regulation of Cyberspace: Singapore

Singapore Computer Misuse Act, 1993 (SCMA) was first introduced in 1993 and has been amended several times. SCMA distinguishes between access to a computer and access to a protected computer for the purposes of calculating penalties. The offences are setup in Part II of the Act. It is a relative short piece

---

\(^6\)Ibid, at 950.  
\(^62\)Ibid, at 608.  
\(^63\)Ibid, at 624.
of legislation. Most of the search and seizure provisions are covered by the need to obtain permission of a Public Prosecutor to exercise the powers granted. In 1998, it underwent amendments and the penalties saw considerable changes, they were increased. Thereafter, Singapore designed its Electronic Transactions Act 1998 around the Model Law.

6.27 Legal Regulation of Cyberspace: Sweden

Swedish government assigned the Post and Telecom Agency to submit a proposal for Internet security. This proposal is based on the Government Bill 2004/05:175: From the IT Policy for Society to the Policy for IT Society. The bill covers all areas of society.

6.28 Legal Regulation of Cyberspace: Taiwan

Information security policy in Taiwan has the four key directions which are as follows:

- establishment of a national security incident monitoring and reporting system for I&C,
- consolidation of national security awareness for I&C and the promotion of information security education,
- standardization and certification services,
- Promotion of international cooperation for preventing cyber crime.

---

6.29 Legal Regulation of Cyberspace: The League of Arab States

Several countries in the League of Arab States have adopted cyber crime legislation, such as Saudi Arabia and United Arabic Emirates. The Gulf Cooperation Council (GCC) involving Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and United Arabic Emirates, has at a conference in June 2007 recommended that the GCC countries make a treaty on cyber crimes.67

6.30 Legal Regulation of Cyberspace: United Kingdom

United Kingdom (UK) cyber crime laws are in the form of the Computer Misuse Act 1990. The Act was enacted by Queen’s most Excellent Majesty, by and with the advice and consent of Lords Spiritual and Temporal, and Commons to make provision for securing computer material against unauthorized access or modifications; and for connected purposes. The Computer Misuse Act created three offences: (i) unauthorized access to computer material, (ii) unauthorized access with intent to commit or facilitate commission of further offences and (iii) unauthorized modification of computer material.

Criticisms of the Act include that68:

- It has been an insufficient deterrent with remarkably few successful prosecutions and lenient sentencing. One view is that the number of successful prosecutions is low because of the difficulties of meeting the requirement to prove intent on the offender’s part.
- It is out of date.

67 Available at www.usdoj.gov/ag/events/g82004/index.html.
Chapter 6  
Legal Regulation of Cyberspace

- It lacks a framework for international co-operation in investigating and prosecuting e-crime.

6.31 Legal Regulation of Cyberspace: United Nations

The United Nations General Assembly has adopted a number of resolutions. General Assembly Resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on “Combating the criminal misuse of information technologies”, are most important. The Resolution 56/121 invites Member States, when developing national laws, policy and practices, to combat the criminal misuse of information technologies, to take into account, inter alia, the work and achievements of the Commission on Crime Prevention and Criminal Justice.\[^{69}\]

*International Telecommunication Union (ITU) in Geneva.*

The most active UN-institution in reaching harmonization on global cyber security and cyber crime legislation is the International Telecommunication Union (ITU) in Geneva. The Secretary-General of the ITU launched in May 2007 the Global Cyber security Agenda for a framework where the international response to the growing challenges to cyber security could be coordinated. GCA is the framework for proposing strategies for solutions to enhance confidence and security in the information society, under the umbrella of cyber security. ITU in Geneva is uniquely positioned for developing a global agreement or protocol on cyber security and cyber crime. It may be then called the Geneva Protocol. In order to assist the ITU’s Secretary-General in developing strategic proposals to Member States, a High Level Experts Group

Chapter 6  Legal Regulation of Cyberspace

(HLEG) was established in October 2007. This global expert group of more than 100 experts delivered Reports and Recommendations in June 2008, and the Chairman’s Report was published in August 2008. The Global Strategic Report was published on November 12, 2008, including strategies in the following five work areas: Legal Measures, Technical and Procedural Measures, Organizational Structures, Capacity Building, and International Cooperation\textsuperscript{70}.

6.32 Legal Regulation of Cyberspace: United States

Both at the federal and state levels, numerous laws have been enacted to address the threat of cyber crime; among these are\textsuperscript{71}:

\textit{Federal Computer Fraud and Abuse Act}

The Act makes it a Federal crime to access a computer without authorization or in excess of the authorization, for the purpose of causing an unauthorized act\textsuperscript{72}.

\textit{The Ribikoff Bill}

In the United States a staff study by the U.S. Senate Government Operations Committee in February 1977 was the first comprehensive initiative on computer crime. The staff study addressed several problems associated with computer programs, and recommended that legislation should be considered that would prohibit unauthorized use of computers. Cryptography export is controlled since 1996 by the Export Administration Regulation of the Department of Commerce, administered by the Bureau of Export

\textsuperscript{70}Available at www.itu.int/osg/csd/cybersecurity/gca.
Administration. The US regulations changed in December 31, 1998, leading to more flexible cryptography export controls to 45 countries.\(^73\)

**The Stanford Draft Convention of 2000**


**Sarbanese Oxley (SoX) Act of 2003**

SoX has many provisions, some of which require management of publicly traded companies to establish and maintain “an adequate internal control structure and procedures for financial reporting” as well as to provide an assessment of the effectiveness of the structure and procedures that have been established.\(^75\).

The US House of Representatives has passed the “Electronic Signatures in Global and National Commerce Act”, HR 1714 or E-SIGN. This legislation is designed to give electronic signatures and records the same legal significance as a written contract.\(^76\)


In US, the White House announced “The National Strategy to Cyberspace Security” as the security blueprint of US government in February 2003. The document continues the work started by the Department of Homeland Security (DHS) for improving homeland security in cyberspace. The scope of this document covers the federal government, state and local governments as well as private sectors and the American people. It outlines five major goals of security: building a national cyberspace security response system, developing a threat and vulnerability reduction system, expanding awareness and training programs, securing the government’s cyberspace, and promoting national security and international cyberspace security cooperation.\textsuperscript{77}

\textit{Organization of American States (OAS)}

In 1999 The Ministers of Justice or Ministers or Attorney Generals of the Americas in the OAS recommended in Peru the establishment of a group of governmental experts on cyber crime.\textsuperscript{78}

\textit{The Electronic Frontier}

The U.S. President established in 1999 a Working Group in order to provide an initial analysis of legal and policy issues surrounding the use of the Internet to commit unlawful acts. The Working Group’s report was called \textit{The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet}, and published in March 2000. The report recommended approaches for addressing unlawful conduct on the Internet.\textsuperscript{79}

\textsuperscript{78} Ibid.
6.33 Issues in legal regulation of cyberspace

The law is an instrument used by government to secure and promote the economic base of a society. Cyberspace is a growing source of legal concern for states, institutions, and individuals. It is evolving rapidly into a highly dynamic space, one that is supportive of varied transactions and interactions. The legal discussion on the rise of law on the Internet has spawned several issues in regulation of cyberspace.\(^8\)

**Issue regarding use of Legislation for regulation of cyber space.**

First and foremost issue is whether Legislation is required or not for regulation of cyber space. Two main views have emerged regarding legal regulation of cyberspace. First are those who advocate tighter government legislation and others are those who see that the cyberspace will create its own rules from the bottom up. The latter view includes the insight that cyber law will not and cannot be uniform but will grow from the different communities into a patchwork of specific laws from specific online communities.\(^8\)

**Issues regarding regulatory model to be adopted for regulation of cyberspace**

The second issue is which regulatory model to be used for regulation of cyberspace Various regulatory models are available in theory: Apart from the possibility of no regulation at all, which cannot be considered as a real “solution”, the choice is principally between traditional national regulation, international agreements and self-regulation. As mentioned, national regulation has the disadvantage of not meeting the globalization needs of an adequate legal framework in view of the fact that transactions through the cyberspace are usually of a cross-border nature. So far, the regulatory model in the cyberspace


\[^8\]Ibid.
Chapter 6  
Legal Regulation of Cyberspace

is based on self regulation through manifold business standards, starting from technical guidelines and leading to fair information practices. Self-regulatory model follows the well-known principle of subsidiary, meaning that the participants of a specific community try to find suitable solutions (structures, behaviors) themselves as long as government intervention has not taken place. The legitimacy of self-regulation is based on the fact that private incentives lead to a need-driven rule setting process. Furthermore, self-regulation is less costly and more flexible than State law. In principle, self regulation is justified if it is more efficient than state law and if compliance with rules of the community is less likely than compliance with self-regulation. The theoretical approaches to the self-regulatory model show a multi-faceted picture: In many cases, self-regulation is not more than a concept of a private group, namely a concept occurring within a framework that is set by the government (directed self-regulation or audited self-regulation). This approach has gained importance during the last decade: if the government provides for a general framework which can be substantiated by the private sector often the term “co-regulation” is used. The state legislator does not only set the legal yardsticks or some general pillars of the legal framework, but eventually the government remains involved in the self-regulatory initiatives at least in a monitoring function supervising the progress and the effectiveness of the initiatives in meeting the perceived objectives.

Issues regarding source of Cyber law

Third issue in legal regulation of cyberspace is that for the establishment of an adequate legal framework there is a need of appropriate legal source. Even if the manifold merits of self-regulation are to be honored, some pillars of the legal framework in the context of security and privacy need to be set by the  

legislator. Since legislation is hardly develop in a fast moving field such as the
 cyberspace, the main legal source is to be seen in the customary rules, general
 principles of law, such as good will, equal treatment, fairness in business
 activities, legal validity of agreements etc. Involvement of the legislator seems
to be inevitable. Such law would have to be introduced on an international
level83.

Contemporary theories addressing international law aspects tend to
acknowledge a wide definition of international law, according to which this field
is no longer limited merely to relations between nation states but generally
accepts the increasing role of other international players such as individual
human beings, international organizations and juridical entities. To some extent,
basic legal principles are considered to be an expression of “natural law”;
practically, general legal principles may be so fundamental that they can be
found in virtually every legal system. The specific problem in view of security
and privacy, however, consists in the appreciation that privacy concerns are not
identical in the different regions of the world which makes the application of
general principles difficult in cross border business activities. Therefore, a basic
legal framework should be introduced by an international legislator; however,
the details of the legal rules for the protection of security and privacy needs are
to be developed by the private sector. The cyberspace being a new system itself,
the idea of entrusting a body with its legislation and governing that is new, too,
is not far-fetched. A new body would be in the position to take into account all
the characteristics of the cyberspace. Furthermore, considering the complexity
of the cyberspace, this body could be construed in a way to dispose of the
necessary capacities84.

for cyberspace. Part 1: Developing rules for transitioning custom into law,” Vol. 26,
84 Y. Akdeniz, “UK Government and the Control of Internet Content,” Vol. 17, Computer
Chapter 6  
Legal Regulation of Cyberspace

Issues regarding difference in pace of development in law and technology

Another issue of great concern is that the development of rules to order and regulate intercourse in the digital world is slower than the pace and development of new forms of communications technology, electronic analogues and legal entities. In fact, due to the speed by which technology evolves and its impact on human behavior and transactions, the problem is magnified manifold in contrast to the pace of developments in the real world\textsuperscript{85}.

Issues regarding conflict of rules

Further, cyberspace is an area currently regulated by a large number of different, but partly overlapping, pieces of legislation. Legislation is enacted, amended and repealed at what seems to be an ever-increasing speed. It is very hard to obtain a sufficient over-all grip on the legislation. Thus there is risk of development of conflict between different sets of rules, regulations, orders etc. Self-regulatory rules may also conflict with government regulations in ‘mixed’ transactions depending on the situation. Adding to the confusion is the fact that one and the same term can be used differently in different legislations (at least in their translated form). This lack of coordination in the terminology is obviously not obstacle for effective application of the legislation. However, it is not just the enormous amount of legislations that cause problems, also the inconsistency in the interpretation of the law is a problem, and this problem is augmented by overlapping agency authority\textsuperscript{86}.

Issue regarding awareness of Cyber law

Regulations are being proposed, discussed, and enacted at a rapid rate. To persons moving their practice into cyberspace, this means that the ground rules

\textsuperscript{85} Ibid.
\textsuperscript{86} Ibid.

198
are rapidly evolving and changing. Because of the changing legal and regulatory floor, people may not stay informed about legislative and regulatory trends so they cannot meet new standards as they are established. Thus a number of issues as described above needs to be addressed before regulation of cyberspace through legal measures become a reality.

6.34 Conclusion

The legal and regulatory framework affecting cyberspace is both complex and rapidly evolving. Since 1995 there have been a number of states that have enacted their own legislation for regulation of cyberspace. These states, however, take divergent approaches which result in inconsistency in the regulations between states. Divergent and fragmentary legislation around the world does not constitute the most suitable environment for regulation of cyberspace and to some extent has created new barriers. Co-operation between national governments is particularly important in this regard and harmonized law is badly needed given the global nature of cyberspace.

The development of information, product and services in cyberspace has not abated and may in fact be accelerating. The rise in the popularity of the cyberspace has created a range of interesting and potentially novel legal problems that will have to work themselves through the system in due course. Hence, it is imperative to make haste to reevaluate the sufficiency and suitability

---

of the existing forms of rule-making, with a view to creating a multi-pronged and more comprehensive and reactionary regulatory solution for cyberspace.\textsuperscript{90}

Inspiration can be sought from recognized sources of law from both domestic and the international legal systems to identify and give recognition to potentially new ones. A framework of substantive key principles set by a legislator at the international level, complemented by the private sector with more detailed regulation seems to be the best solution. Through such a framework, general pillars of regulation could be set for everyone, which are then suitable to be supplemented by the individuals concerned in a way that suits their current needs. Furthermore, the inclusion of an international legislator in the process also ensures the continued involvement of the public sector, contributing at least by monitoring the process. The approach chosen by the European Commission goes in that direction. However, it would be preferable to have an international (not European) legislator setting the framework; such an approach would better adapt to the needs stemming from the globality of the cyberspace. Furthermore, if a more detailed regulation should be established by the private sector, lessons can be drawn from Internet governance in general, where the private sector has already marked presence in the rule setting.\textsuperscript{91} While according mechanisms still need to be developed, the early recognition of eventual problems and suggestions for their encounter leaves hope that effective legal regulation can be established before cyberspace is in full operation.
