Expert Meeting on

CYBERLAWS AND REGULATIONS FOR ENHANCING E-COMMERCE: INCLUDING CASE STUDIES AND LESSONS LEARNED

25-27 March 2015

The ESCWA Cyber Legislation Digest

By

UN-ESCWA

United Nations Economic and Social Commission for Western Asia

UN-ESCWA
UNITED NATION ECONOMIC AND SOCIAL COMMISSION FOR WESTERN ASIA

The ESCWA Cyber Legislation Digest

Development Account Project

Regional Harmonization of Cyber Legislation to Promote Knowledge Society in the Arab Region

United Nations

New York, 2013

ACKNOLWEDGEMENTS

This digest summarizes the ESCWA activities between 2007 and 2012 in the area of cyber legislation. It is published by the Information Communication Technology Division at the United Nations and Social Commission for Western Asia (ESCWA) within the framework of its project “Regional Harmonization of Cyber Legislation to build Knowledge Society in the Arab World”.

The preparation of this digest was supervised by Ms. Nibal Idlebi, the Chief of the ICT Applications Section, and the manager of the Cyber Legislation project. Mr. Syed Ahmad, the associate IT officer, contributed to the peer-review and the enhancement of this report. The commission gratefully acknowledges the contribution of Mr. Akram Najjar, a consultant in the field of Information Communication Technology, who prepared this report based on the ESCWA activities.

Table of Contents

Note: This document has been reproduced in the form it was received without formal editing. .

1.0 Executive Summary

This digest aims to inform its readers about ESCWA's cyber legislation initiative specifically those activities relating to the Harmonization Project.

In 2007, ESCWA launched its cyber legislation initiative. This resulted in a set of activities that served to regularize the approach for implementing cyber legislation in the Arab world, at the national and regional levels. This initiative focused on a project called '**The Regional Harmonization of Cyber Legislation to Promote the Knowledge Society in the Arab World'**. In this digest, this project is referred to as the '**Harmonization Project'** and covers all ESCWA activities from 2007 to present.

The approach taken by ESCWA in this project was based on a deep involvement with key stakeholders: legal country representatives, ICT consultants, representatives of various international organizations and other concerned bodies. It was through such collaboration that ESCWA developed the cyber legislation templates and directives, which are currently being implemented in various ESCWA member countries.

Having assessed the status of cyber legislation in the region, ESCWA started by developing a document called the '**Models for Cyber Legislation'**. This document provided a situational analysis of cyber legislation in the member states of ESCWA, and made recommendations on how to address and implement cyber legislation.

ESCWA then developed six **templates** for the definition of cyber legislation. These templates identify general areas of concern that should be addressed by every country embarking on introducing robust cyber legislation and regulations, and consist of a set of headings broken down hierarchically. The templates serve as a model for the analysis of cyber legislation in each country and as a tool for developing legislation where it is lacking. ESCWA used the templates to evaluate cyber legislation in Bahrain and in Syria.

Based on the **model** and the **templates**, ESCWA developed six directives. Each directive addresses a key issue in cyber legislation, such as e-Communication, Freedom of Expression, Cybercrime, etc. For each directive, ESCWA analyzed the situation in the Arab region, defined the scope of issues addressed by the directive and most importantly, developed a proposed set of Sections and Articles to be used in the drafting of cyber legislation.

To support its cyber legislation activities, ESCWA developed a **cyber legislation portal**. It also developed and launched a **virtual network** for the ongoing support of cyber legislation stakeholders in the Arab region.

Building on these outputs, the digest presents a set of **recommendations** for continuing efforts to improve cyber legislation in the ESCWA region.

Finally, the digest summarizes the **process and methodology** ESCWA used in developing and implementing the cyber legislation initiative.

2.0 The Context for Cyber Legislation in the ESCWA Region

2.1 The Importance of Cyber Legislation for Building a Knowledge Society

Technological advancement is an important socio-economic issue for the ESCWA region. Countries with developed economies are currently diversifying from their reliance on commodities and moving into knowledge-based economies. Developing countries also need to pursue such a path. The development of a knowledge based society depends heavily, if not entirely, on technological enablers for efficient development. These enablers are necessary for the development and implementation of various technological facilities such as electronic commerce, communication and the use of the Internet.

In the past 10 years or so, there has been a significant increase in PC, mobile and internet penetration in ESCWA member countries. This growth enabled these countries to recognise the potential of the Internet as a source of progress and development. It has also been generally accepted that web-based activities in the region cannot flourish without a proactive and favorable environment for their use, by people in their various activities.

2.2 The Scope of Regulation

To provide such an environment implies the regulation of the virtual space covered by the Internet, commonly referred to as **cyberspace**. This is a global space unattached to any geographical or jurisdictional scope. It therefore becomes necessary to regulate cyberspace without hindering progress and development.

The legal foundation and framework used to regulate cyberspace is generally referred to as **cyber legislation**. This is a virtual world that manages the legal aspects of issues as wide as personal data, electronic transactions, intellectual property and others. It covers the creation of laws for the components and activities in cyberspace.

Given that no single country has jurisdiction over such an international domain, cyberspace is difficult to regulate. However, regulating national cyberspace is possible, and requires the development of an appropriate legal foundation and framework. Since legislation has always lagged behind the development of technology, such a foundation becomes even more urgent.

Regional cyberspace can be regulated when countries enter into relevant conventions and agreements. These can define the online dealings of computer system users, electronic communications and the Internet across borders. Such dealings would provide incentive for these countries to develop their knowledge societies. If on the other hand, cyberspace is left unregulated, users will be discouraged from undertaking cyber transactions which would inevitably hinder socio-economic development.

2.3 The Status of Cyber Legislation in the ESCWA Region

The Arab region has already ventured through various initiatives that introduced some cyber laws and regulations. All Arab countries agree on the importance of cyber legislation, specifically as this feeds into the regional strategies and plans launched to prepare for a regulated ICT environment favorable to the most suitable usage of cyberspace.

Cyber legislation in the ESCWA region started with the issue of the electronic transactions law in the Kingdom of Jordan, in December 2001. This was followed by a United Arab Emirates law specific to the exchange of information and electronic commerce in February 2002. The Kingdom of Bahrain introduced an electronic commerce law in September 2002.

Cyber legislation was also considered an important issue, though not addressed comprehensively, in two key initiatives:

- The ESCWA Regional Plan of Action[1] (RPoA) developed in 2005 as an overall umbrella which outlined all actions needed to build the Information Society including cyber laws as part of the World Summit on the Information Society (WSIS);
- The Arab ICT Strategy [2] developed by the League of Arab States for the region and for the period 2007 to 2012.

There was a lull in cyber legislation activities until March 2007, when the Kingdom of Saudi Arabia issued a law addressing electronic transactions followed closely by a similar law in the Sultanate of Oman in May 2008. After that, most cyber legislation activity was prompted by the initiatives of ESCWA, as discussed in this digest.

In recent years, there have been a few laws aimed at improving the status of knowledge societies in the Arab region. The most recent were:

- The electronic transactions law issued by Qatar (2010);
- The cybercrime law in the Kingdom of Jordan (2010);
- The e-Signature and network services law (2011) as well as the law to cover cybercrime issues in Syria (2012)

Some countries such as Algeria and Morocco took the approach of introducing laws to protect intellectual property by modifying and updating their existing intellectual property laws.

ESCWA prepared six tables showing the cyber legislation implemented by each ESCWA member country. Each table deals with a certain key area of cyber legislation. These key areas correspond to the six directives developed by ESCWA (see Section 3.5).

[1] http://isper.escwa.un.org/RegionalActionPlans/RegionalPlanofAction/RPoADocument/tabid/68/language/en-US/Default.aspx
[2] http://isper.escwa.un.org/RegionalActionPlans/ArabICTStrategy/StrategyDocument/tabid/70/language/en-US/Default.aspx

The Status of Cyber Legislation on Key issues

e-Signature Laws: These can be considered as the most commonly implemented laws in the Arab world. Countries that have already issued such laws include: the United Arab Emirates, the Kingdom of Jordan, the Kingdom of Bahrain, Tunis, Algeria, the Kingdom of Saudi Arabia, Syria, the Sultanate of Oman, Qatar, Egypt and Morocco.

e-Transactions and e-Commerce: laws related to e-Transactions are well developed in the Arab world. As for e-Payments, the ESCWA region has not yet covered such issues, with the exception of Lebanon and Yemen. In Lebanon, the central bank issued various decrees related to the regularization of electronic payments and exchange. Additionally in Yemen, a special law was issued to cover electronic banking transactions.

Figure 1 shows the status of individual Arab countries as far as electronic transactions, e-Signature and e-Commerce laws are concerned.

Figure 1: Status of e-Signature, e-Transaction and e-Commerce Laws in selected Arab countries

Country / Law	e-signature	e-transaction	e-commerce
Algeria	Draft law	Draft law	Draft law
Bahrain	Yes, Law 28/2002	Yes, Law 28, 2002	Yes, Law 28, 2002
Egypt	Yes, Law 15/2004	Draft Law	Draft Law
Iraq	Yes, Law 78, 2012	Yes, Law 78, 2012	Yes, Law 78, 2012
Jordan	Yes, Law 85/2001	Yes, Law 85/2001	..
Kuwait	Draft Law	Draft Law	..
Lebanon	Draft Law	Draft Law	Draft Law
Libya	..	..	..
Morocco	Yes, Law 53-05/2007	Yes, Law 53-05/2007	Yes, Law 53-05/2007
Oman	Yes, Law 69/2008	Yes, Law 69/2008	..
Palestine	Draft Law	Draft Law	..
Qatar	Yes, Law 16/2010	Yes, Law 16/2010	Yes, Law 16/2010
Saudi Arabia	Yes, Law 18 /2007	Yes, Law 18 /2007	..
The Sudan	Yes, 2007	Yes, 2007	Yes, 2007
Syrian Arab Republic	Yes, Law 4/2009	Draft Law	Draft Law
Tunisia	Yes, Law 83/2000	Yes, Law 83/2000	Yes, Law 83/2000
United Arab Emirates	Yes, Law 1/2006	Yes, Law 1/2006	Yes, Law 1/2006
Yemen	Partly, e-payment law 40/2006	Partly, e-payment law 40/2006	..

Source: Reports of the ESCWA project on cyber legislation
http://isper.escwa.un.org/FocusAreas/CyberLegislation/Projects/tabid/161/language/en-US/Default.aspx

Protection of Personal Records: this has not been addressed at all in the ESCWA region, except for the Emirate of Dubai in the United Arab Emirates. As for countries in North Africa, both Tunis and the Kingdom of Morocco have issued such laws. This is a key issue as the protection of personal records is critical while implementing e-Government and e-Commerce.

Consumer Protection: there has been a lack of progress in this area, with the exception of Tunis and Lebanon. Both countries have issued general laws that cover consumer protection which also address protection in cyber space.

Laws to Combat Cybercrime: This is a commonly addressed area. These have seen quick implementation in countries such as: the United Arab Emirates, the Kingdom of Saudi Arabia and the Sudan. Other countries have draft laws or bills such as the Kingdom of Bahrain, Algeria, Syria, the Sultanate of Oman and Egypt. Tunis and Morocco have found it more suitable to include articles related to cybercrime under their own laws of electronic commerce and intellectual property.

Figure 2 shows the status of individual Arab countries as far as cybercrime is concerned.

Figure 2. Adoption of Cyber Crime Laws in selected Arab countries

Country	Specific Law for Cyber crime	Year
Bahrain	Law 28 on e-Transaction includes articles related to cyber crimes	2002
Egypt	Ministerial Decree No. 327 on the establishment of the Department Detectives combat Internet crimes Computers	2005
Jordan	Law 30 on Information System crimes	2010
Kuwait	Draft Law on combating Internet crimes	
Lebanon	Circular No. 4 on the protection of software programs and the fight against piracy	2006
Morocco	Law 53-05 on Electronic Exchange of legal Data includes articles related to cyber crimes	2007
Oman	Royal Decree 27 to amend the Penal code and adding article 276 on Computer crime	2001
Palestine	Draft amendment of penal Code to include articles on cyber crimes	
Saudi Arabia	Law 79 on Combating Information Technology Crime Law	2007
The Sudan	Law 14 on Information Technology Crimes	2007
Syrian Arab Republic	Law 17 on Regulating communication on the net and combatting cybercrime law	2012
Tunisia	e-transaction and e-commerce law includes articles related to cyber crime	2007
United Arab Emirates	Federal Law 2, Combating cybercrime law	2006
Yemen	Draft Law on combating electronic crimes	

Source: Compiled by ESCWA, refer to: **http://cyberlegislation.escwa.org.lb/sites/default/files/download/Dir-5-Cybercrimes.pdf**

Intellectual Property Protection: Most countries have favoured updating their existing intellectual property laws to include cyberspace related aspects of such protection. However, a comprehensive set of cyber legislations related to intellectual property (including those aspects related to databases) have yet to be addressed in the Arab world.

2.4 Limitations in the Implementation of Cyber Legislation

Despite some Arab countries having issued numerous laws for cyberspace, the following criticisms still remain:

- Most of these countries did not allow for an integrated package of laws that fit under the proper scope of cyber legislation;
- They did not have a comprehensive set of laws that cover various foundations of ICT operations;
- There have been few regional initiatives or special projects under cyber legislation;
- Coordination and regional integration of cyber legislation was found lacking;
- There are wide gaps between in the maturity of cyber legislation in the region. For example, the Kingdom of Bahrain has implemented various laws and regulatory decrees related to electronic transactions and commerce as well as the protection of intellectual properties, yet countries like Iraq and Kuwait have not addressed these issues at all, despite them having draft laws that have not been implemented yet;
- Most countries in the region have not covered the legal aspects of electronic payments with the exception of Lebanon and Yemen;
- Most countries in the region have also not covered the issues of consumer protection in cyberspace with the exception of Lebanon and Tunis;
- Most countries in the region have not covered issues of personal data protection in cyberspace.

In the workshop conducted by ESCWA in Cairo (March 2012), Dr. Younes Arab presented the paper "Applying ESCWA Cyber Legislation Directives". This document provides a useful overview of the potential obstacles to a comprehensive implementation of cyber legislation in the Arab world[3].

[3] http://isper.escwa.un.org/FocusAreas/CyberLegislation/Projects/tabid/161/language/en-US/Default.aspx

3.0 The ESCWA Cyber Legislation Initiative

Prior to 2007, extensive studies and regional analysis on cyber legislation was conducted in areas of the world outside of the ESCWA region. Comparable material was not available for the ESCWA region with few attempts made at developing cyber legislation in a concerted and planned manner.

The nascent nature of knowledge societies in most ESCWA member countries required immediate legislative action, in order to create an adequate enabling environment for ICTs to flourish. Without a catalytic and conjoined effort to support their legislative plans, policymakers were not well prepared in addressing cyber legislative issues. Resolving these issues is of great importance towards facilitating electronic interactions between ESCWA member countries and at the Arab regional level.

Most developed countries, as well as some developing countries, have recently started to update or have already updated their legal and regulatory frameworks, in line with the needs to adopting new technologies. An example is the launch of the "e-Europe Initiative" by the European Commission (2000), which aimed at accelerating Europe's transition towards a knowledge-based economy[4]. This would then realize the potential benefits of higher growth, more jobs and improved access for all citizens, to the new services of the information age.

A similar effort was needed for the ESCWA region in particular and the Arab world in general. In 2007, ESCWA commenced with a series of activities aimed at the **Regional Harmonization of Cyber Legislation to Promote the Knowledge Society in the Arab World**.

In launching **Regional Harmonization** activities, ESCWA aimed at enhancing the regional integration of cyber legislation. It also aimed at strengthening the capacity of member countries to develop their own knowledge societies. These two aims need to be achieved by building a strong and sustainable ICT sector supported by appropriate legal and regulatory frameworks. Such suitable frameworks lead to growth in the regional economy, particularly in the ICT sector, through the implementation of appropriate laws.

3.1 The Objectives of Cyber Legislation

The general objectives of cyber legislation were understood by ESCWA as follows:

1. To prevent the illegal use of cyberspace.
2. To provide a framework that allows judiciary processes to address cybercrime when it happens.
3. To reinforce human rights by recognizing the variety of aspects that relate to the digital rights of individuals.
4. To enhance the different modes of electronic communication by providing the required traceability, security and protection of data.
5. To define in clear terms the obligations, liabilities and responsibilities of all stakeholders.

[4] http://ec.europa.eu/information_society/eeurope/i2010/archive/eeurope/index_en.htm

6. To promote the use of ICT applications and e-Services in governmental, economic, social and cultural activities so that users become more confident conducting online transactions.

These general objectives were converted to more specific objectives for the Harmonization Project as shown in the next section.

3.2 The Objectives of the Harmonization of Cyber Legislation

Following on from the above objectives, ESCWA established the objectives and expected achievements (see next section) as follows:

- To enhance regional integration in the field of cyber legislation and Knowledge Societies.
- To strengthen the capacity of member countries to develop their knowledge societies through the drafting of cyber legislation.
- To build a strong and sustainable ICT sector in member countries through the development of appropriate legal and regulatory frameworks.

Such objectives will lead to growth in the region's economy, particularly in the ICT sector, by:

- Facilitating e-Transactions between the countries of the region with the removal of legislative contradictions that may otherwise hinder their completion.
- Enhancing regional and cross-border business and trade as extra-national consumers will be less concerned about falling into legislative vacuums.
- Minimizing ICT market segmentation problems and increasing cross-border competitiveness by enabling access to wider markets for businesses which would otherwise find it difficult to sell and expand outside of their national borders.

Various activities and results were accomplished starting with the development of the Cyber Legislation Model, going through the approval of the Harmonization Project in 2008 and launching it in 2009. The project is currently being conducted by ESCWA's Information and Communication Technology Division (ICTD).

3.3 Models for Cyber Legislation in ESCWA Member Countries

ESCWA's cyber legislation efforts began in 2007 as a project for the harmonization of cyber legislation in ESCWA member countries. This was followed by a study entitled '**Models for Cyber Legislation in ESCWA Member Countries'.**[5] This study formed the basis of the approach to the harmonization of cyber legislation. It justified the launch of the harmonization of cyber legislation and prepared the ground for implementation activities in the region.

[5] http://www.escwa.un.org/information/publications/edit/upload/ictd-07-8-e.pdf

This study was discussed in a peer review meeting in 2007 and a meeting was set up to discuss the Model and review its findings (details can be found in Appendix B: Timeline). The study was presented with two major objectives.

First Objective: Situational Analysis

The first objective was to present a review of the status of cyber legislation in the region. This covered several areas of analysis including:

1. A survey of legal texts, international conventions, directives, treaties and national laws of selected countries.

2. A review of cyber legislation activities in the ESCWA region. This included full legal texts and articles of laws on such cyber-related topics such as e-Commerce, consumer protection, intellectual property and e-Transactions.

3. Ratifications made by ESCWA member countries to international conventions were outlined.

4. An analysis of current cyber or cyber related legislation in the ESCWA region, in terms of whether such laws exhausted all topics as compared with international conventions and non-Arab cyber laws.

Second Objective: Recommendations

The second objective was to present recommendations for drafting model cyber laws in the ESCWA region. This was crucial as most ESCWA member countries still lack such legislation. Such a lack can be attributed to reasons such as:

- an underestimation of the importance of and the need for such legislation;
- the judicial bodies in some countries not having a significant enough backlog of cyber related cases to cause concern;
- countries have not been able to use existing laws and provisions by analogy and through broad interpretation in order to adjudicate cases dealing with cyberspace.

The document presented the following recommendations:

1. Identification of the cyber legislation topics to be addressed as:

    - Data protection;
    - Cybercrime;
    - Censorship and freedom of expression;
    - Privacy on the Internet;
    - E-Commerce;
    - Telecommunications.

    These were used to develop ESCWA's six directives (see Section 3.43.5).

2. The second step was to assess the status of legislation in each ESCWA member country. This would result in identifying gaps between what is present and what is required. Legislators can then opt for one of three approaches:

   - Drafting local laws;
   - Ratifying international treaties;
   - Adopting a model law available on a regional or international level.

3. A mechanism was proposed for enacting the new laws and consisted of the following activities:

   - Creating specialized focus groups: of concerned ministries, ICT experts and legal professionals in cyber legislation.

   - Based on the recommendations of the focus groups, model laws would be defined, discussed and enlarged to include laws that were hierarchically broken down into specific sections and articles.

   - Interviews and workshops would then be conducted to discuss the laws, acquaint key stakeholders with these laws, address issues of compliance with existing laws, subsequently, laying the groundwork for eventual implementation.

   - The final phase, before enacting the laws, would include discussion sessions concerning the draft laws. The aim of these sessions is for stakeholders to ensure that the draft laws cover all possible situations.

The importance of these recommendations directly led to the need for regional harmonization amongst ESCWA member countries.

3.4 The Six ESCWA Cyber Legislation Templates

The first step towards the harmonization of cyber laws in the ESCWA region was the development of **six templates** during 2007 and 2008. The six templates include a set of headings broken down hierarchically. The headings identify areas of cyber legislation concern, to be addressed by every country embarking on the introduction of robust cyber legislation and regulations.

The templates can be used as follows:

- To identify the breakdown of the various issues of each of the six areas of a directive and hence use such a hierarchical breakdown for addressing the issues nationally.
- To evaluate the status of a country vis-à-vis cyber legislation.

ESCWA applied this template for two member countries (Syria and the Kingdom of Bahrain) and prepared reports summarizing their findings.

The Definition of Templates

ESCWA developed the cyber legislation templates as tools which could help ESCWA member countries in formulating new cyber laws and/or the evaluation of their existing national cyber laws. There are six templates, each one covering one of the main areas for the enhancement of the regulatory framework for cyberspace. Each template includes components and sub-components for the development or adaptation of cyber legislation.

The templates focus on principles, issues, areas of high concern and matters relating to the directive. By comparison, the six directives offer more concrete, specific proposals: chapters, sections and articles to be used while developing cyber legislation. The six templates are available on the webpage referred to in the link below.[6] The directives are discussed in the Section 3.5.

The Background and Current Status of the Templates

The development of the templates started in 2007 and was based on several sources, such as:

- Various international and regional conventions and agreements i.e. the Combating of Cybercrime by the European Union.
- The model laws and rules of the United Nations Commission on International Trade Law (UNICITRAL).
- National laws and regulations of some countries such as France's laws on the protection of personal data.

The templates were announced during the December 2008 workshop conducted by ESCWA (see Appendix B). They were first used to analyses the status of cyber legislation in the Kingdom of Bahrain and in Syria in the same year.

By 2010, ESCWA had achieved the introduction of the templates in the Arab region, which are currently being implemented. The status of these countries is described in six tables corresponding to each directive. Each table contains a list of ESCWA member countries, and the specific parts of the templates that have been implemented in those countries.

3.5 The Six ESCWA Cyber Legislation Directives

The six directives represent the core of the cyber legislation initiative's output. They consist of sample laws expressed as chapters, sections and articles. For a detailed explanation of the methodology used to develop these directives, please consult Section 5: Process and Methodology.

The package of six compatible directives was developed in Arabic as six separate documents. They have also been published as one consolidated document.

[6] http://isper.escwa.un.org/FocusAreas/CyberLegislation/Template/tabid/201/language/en-US/Default.aspx

Each of the six documents has the following structure:

- The areas that ESCWA's research covered, essentially the scope of the directive.
- The experience of ESCWA member countries in formulating legislation related to the directive and a comparison of these formulations with international legislation.
- A descriptive explanation of the proposed laws.
- The specific chapters, sections and articles of the laws proposed for the specific directive.

Additionally, each document referenced a wide range of studies, laws or cases relating to the subject of the specific directive.

These directives were discussed and agreed upon during an expert group meeting that was held at ESCWA's premises in Feb 2011, as detailed in Appendix B.

The directives (together with annex and glossary) are available to download from ESCWA's website[7].

Directive 1: e-Communication and Freedom of Expression

This first directive has a fundamental importance specifically as it forms the basis for other cyber legislation directives. This is due to its handling of the technical and operational aspects related to the determining the identities and responsibilities of the parties that provide electronic communications services. The identities of responsible parties needs to be legally determined after any transgression, hence the legitimation of the various aspects of electronic communication are necessary.

An increase in Internet penetration and broadening in the nature and variety of users goes in parallel with the increase in the types of devices used for accessing the Internet i.e. laptops, mobiles, PCs, tablets, etc. Electronic communication witnessed a shift in paradigm, from being solely used for accessing information to being used as the basis for interactive socio-economic development. This brought to the forefront, the issue of validity of such usage, where any transgression encountered by the transferred information, in terms of medication, blockage, divulging of personal data, may result in damages to various parties involved in the transfer. More importantly, the judiciary world has opened up to the possibility of using such information as legal evidence, requiring firm and legal establishment of the identities of the parties involved, the time and date of transfer and the information systems it was sent from.

Communicators of information that use electronic means have traditionally resorted to various technical devices to protect themselves. These devices resulted in a variety of practices which could be discretionary, illegal, impractical, incomplete or lacking in exposing the identities involved. These incongruous methods were seen as insufficient to protect the public from the misuse of electronic communications.

The issues researched and addressed by this directive include:

[7] http://isper.escwa.un.org/FocusAreas/CyberLegislation/Projects/tabid/161/language/en-US/Default.aspx

1. Electronic data transfer to and from the public and various providers. The directive focuses on the freedom of such transfers and any constraints imposed on it. It also addresses the role of the network service providers and data hosting service providers during such transfer.

2. The legal framework for network service providers in as much as it covers their obligations, liabilities and responsibilities. This also covers their coordination with security and judiciary authorities as regards legislative issues.

3. The encryption of data and the usage of encryption tools, their import and their export. This also covers the responsibility of the providers of such tools as far as the privacy of information is concerned, and the cases where information can or cannot be divulged based on court decisions. Finally, this issue covers the responsibility of providers for the safekeeping of confidentiality of such data.

4. The surveillance of personal and private communications covers cases where surveillance shall be disallowed. Also covered are those cases where such surveillance can be officially allowed.

5. The legal proceedings, particularly penal proceedings, resulting from the transgression of the above laws.

This directive was developed as a comprehensive set of laws that cover telecommunications and freedom of expression. ESCWA relied on the European laws issued in 2000 for electronic commerce as well as the corresponding French laws issued in 2004 and related international and regional laws.

This directive identifies five chapters as follows:

Chapter 1: General Provisions
Chapter 2: The Legal Framework for the Network Service Providers
Chapter 3: Data Encryption
Chapter 4: Electronic Surveillance on Private and Personal Communications
Chapter 5: Criminal Provisions

Their related sections and articles are listed in Appendix A.

Directive 2: e-Signature and e-Transactions

The need for electronic signatures arose after both private and public sector started providing electronic transactions via the web or through direct transacting. This was particularly crucial in the financial sector. The development of various technological means of applying electronic signatures to electronic transactions resulted in the need for a solid legislative framework to safeguard such transactions and provide the necessary certification levels for them.

This directive is concerned with two aspects of e-Signatures and e-Transactions. On the one hand, there is the legal aspect of their use. On the other, there is the technological aspect related to such facilities as encryption systems, public and private key etc.

The issues researched and addressed by this directive include:

1. Electronic signature, records and evidence. This covers regular and official records as well as copies thereof. It also covers the specification of legal conditions that define the authenticity of electronic records and their use as evidence. Also addressed are the data elements and mechanisms to be used when using electronic signatures.

2. The duties and responsibilities of the certification service provider or the owner of the certification and the relying party. This also covers the regularization of the procedures to be followed when issuing authenticated certificates.

3. Legal recognition of countries outside the Arab region of electronic certification. This also considers the issues resulting from authenticated certificates issued outside the Arab region.

4. Financial and banking transactions which covers all types of payment and transfer orders, banking cards and automated withdrawals as well as electronic cash and checks. Also addressed are the specifications of the information systems used for such transactions and the responsibilities of the banks and financial institutions that deal with such transactions and their obligation to safeguard the interests of their clients.

Work was distributed under two sections. The first dealt with the legal aspects of electronic transactions. The second dealt with the technological aspect specifically addressing encryption systems, the use of public and private key as well as the identification of authentication providers within European countries.

This directive identifies five chapters as follows:

Chapter 1:	General Provisions
Chapter 2:	Electronic Records and Signatures
Chapter 3:	The responsibilities of Authentication Service Providers, the owner of the certificate and the relying party
Chapter 4:	Legal recognition of Authentication Certificates issued in Countries outside the Arab Region
Chapter 5:	Banking and Financial Transactions

Their related sections and articles are listed in Appendix A.

Directive 3: e-Commerce and Consumer Protection

Over the past thirty years, commercial transactions occurred through direct or web based connectivity. This consisted of the transfer and acceptance of documentation, electronically such as invoices, payments or transfer orders, contracts and financial statements. The

resulting environment was called e-Commerce (often termed the virtual marketplace or e-marketplace). Transaction volumes, user counts and the number of commercially based websites rose exponentially, and are still rising.

With the rise of competition and the need to reach customers faster, consumers were often left in a vulnerable situation. This was exacerbated by cross-border commerce often resulting in conflicting legal requirements.

The need for a "virtual" legal framework as robust as the traditional paper based laws and regulations became crucial for the progress and development of the international marketplace.

The issues researched and addressed by this directive include:

1. Electronic commercial messages and communications. This covers the use of electronic mail and notifications including their source and date-time stamps. Also covered are issues related to spamming as well as laws that protect consumers using such facilities.

2. Electronically based contracts. This covers issues related to the legal recognition of such contracts as well as issues related to electronic messages used when developing such contracts. Also addressed are issues related to the price fixing and allowing consumers to cancel transactions.

3. Codes of conduct and resorting to non-judiciary resolution of disputes and judicial recourses, such as web based arbitration or rulings.

This directive identifies four chapters as follows:

Chapter 1: General Provisions
Chapter 2: Commercial Electronic Messages and Letters
Chapter 3: Electronic Contracts
Chapter 4: Final Provisions

Their related sections and articles are listed in Appendix A.

Directive 4: The Processing and Protection of Personal Data

With growing concern over human rights, the private and personal data of individuals has naturally become a topical issue. This has been further emphasized by progress in cross-border global communications, the ability of such supporting systems to store and exchange large amounts of data and the increasingly obvious commercial value of such data.

One of the earliest laws covering the processing and protection of personal data was issued in France in 1987. It was later expanded and adopted by the European Council in 1981.

The need for a legal framework to protect individuals and regularize the processing of their private and personal data was one of ESCWA's main concerns.
The issues researched and addressed in this directive include:

1. The general conditions required for the legal processing of personal electronic records. This addresses issues related to the definition of what constitutes a personal record and the principles that allow for its processing. Also addressed are the responsibilities of those parties who are processing such records and the rights of the person whose data is being processed, in order to know what is being processed and how.

2. The setup of suitable control agencies whose main concerns are the protection of electronic personal records. Such agencies will be responsible for the protection of all such records as well as the control of the processing of such records and the authorization for their processing. Such agencies will also have the authority to issue penalties in case of transgressions or improper access as well as blocking access to specific records or halting their processing.

3. Judicial recourses, responsibilities and sanctions. This covers the rights of the owners of personal data to refer to special courts regarding the processing of such personal records. Also addressed are issues related to compensation in the case of transgressions and the cases where such transgressions are allowed by law.

4. The transfer of personal data to countries outside the Arab region. Issues such as the responsibilities of the parties conducting such transfers are addressed as well as the various assurances of such parties to the owners of the safety and security of their records as part of the individual's rights.

5. Codes of conduct covering articles required to regularize rules that can be used to control the protection of personal records.

This directive identifies seven chapters as follows:

Chapter 1: General Provisions
Chapter 2: The Official Control Agency
Chapter 3: General Conditions for the Processing of Personal Data
Chapter 4: Judicial Recourses, Responsibilities and Sanctions
Chapter 5: The Transfer of Personal Data to Countries outside the Arab Region
Chapter 6: Code of Conduct
Chapter 7: Final Provisions

Their related sections and articles are listed in Appendix A.

Directive 5: Cybercrime

With the exponential increase in the penetration of laptops, mobiles and easily accessible networks, a paradigm shift resulted in the generation of a new form of crime, aptly called cybercrime. Gone is the need for criminal equipment and instruments. Any individual with sufficient competence can be party to a wide range of crime categories using ICT facilities. The nature of crimes can also be moral, financial, vandalistic and based on blackmail. The range of crimes is complex and vast making it resistant to counter development using ICT

information systems. Pirating media, pornography, harassment, malware cannot be easily stopped.

The required legal framework needs to define the crimes in specific terms and formulate relevant sanctions.

In general, cybercrime can be categorized into crimes that use the computer as the criminal instrument, the means towards the crime and those crimes where the computer systems, networks or facilities are the target of the crime.

The issues researched and addressed by this directive include:

1. Crimes whose target is data and information and information systems. This covers the misuse of such systems through illegal access, acquisition or distribution of such systems or software or their related passwords or access credentials.

2. Financial crimes covering the use of methods which aim at illegal financial benefits. These cover swindling, embezzlement, illegal promotion or dissemination, the acquisition of passwords, identity theft and access and dissemination of private and confidential data. Crimes related to the misuse of banking cards and electronic money can also be grouped under financial crimes.

3. Sexual abuse of minors: the dissemination of images, text or video clips or incitement to pornographic activities.

4. Infringement of intellectual property: the fraudulent assumption of authorship, imitation of signatures or stamps, copying of electronic documents or the piracy of software products, the sale and promotion of such products and the infringement of intellectual rights.

5. Crimes that misuse personal data. This covers issues related to the processing of personal data without prior authority as well as the divulging of such information.

6. Hate crimes and crimes against humanity through the use of Information Systems. Hate crimes include the publication and dissemination of racial information, threats to or attacks of persons based on their race, colour or beliefs. The denial or distortion of genocide and crimes against humanity are also addressed. Crimes against humanity include the promotion of genocidal activities and incitement to genocide.

7. Promotion and facilitation of drugs and gambling through the use of Information Systems as well as the promotion of alcoholic beverages to minors.

8. Crimes against public and national security using Information Systems: the disruption of governmental activities through the use of Information Systems, the failure of reporting or the misreporting of cybercrimes, access to classified information, illegal manipulation of evidence, its destruction or hiding as well as any terrorist activities or incitement to homicide.

9. Crimes involving the promotion, import or export of encryption tools without license or prior authorization from the required official agencies in the country. Also included is the sale of unlicensed tools.

This directive identifies eleven chapters as follows:

Chapter 1: Crimes whose target is Data
Chapter 2: Crimes whose target is Information Systems
Chapter 3: Misuse of Information Systems and Software
Chapter 4: Crimes of a Financial or Transactional Nature
Chapter 5: Cybercrimes against Minors
Chapter 6: Infringement of Intellectual Property Rights
Chapter 7: Crimes related to Banking Cards and Electronic Money
Chapter 8: Crimes against Private Data
Chapter 9: Racial Crimes or Crimes against Humanity
Chapter 10: Drug and Gambling related crimes
Chapter 11: Cybercrimes against Public and National Security

Their related sections and articles are listed in Appendix A.

Directive 6: Intellectual Property Rights in ICT and Cyberspace

The rise in the penetration of computers led to a wider area of usage than they were originally designed for. Authors, composers, film producers and developers of content, among others, found themselves faced with an ever improving set of tools and utilities to use when developing or creating their works. Works were developed in digital format and often, disseminated in that form.

As in the other five directives, the rise in digital facilities used through Information Systems necessitated the generation of a new set of legislation frameworks, needed to protect the rights of authors against various transgressions.

The issues researched and addressed by this directive cover the legal protection of various items. Legal protection in this directive covers both intellectual property rights as well as the protection of patents. The following include the various areas addressed in the directive:

1. Application software (system and operating software, programming languages, application software, etc.) This covers the legal protection of such products in terms of their ownership, the rights of the holder of the intellectual copyright as well as the exceptions that might result thereof.

2. Databases (content and structure). This covers two aspects: ownership and the right to use such databases.

3. Semiconducting products. This covers laws related to the protection of the owner of such products, those related to the patenting and duration of rights as well as rights related to the topographies of semiconducting products.

4. Digital products other than application software. This covers all regulations concerned with the protection of such products which are not included in the categories of software, databases and semiconducting products.

5. Domain names. This covers the rules and regulations for the issuing of names by suitably assigned authorities, the processes required for the financial and administration processes required for the registration of such domains, their modifications and cancelations. Also addressed are the regulations needed for the resolution of conflicts resulting from the use of domain names.

This directive identifies seven chapters as follows:

Chapter 1: General Provisions
Chapter 2: The Legal Protection of Software
Chapter 3: The Legal Protection of Databases
Chapter 4: The Legal Protection of Semiconducting Products
Chapter 7: Common Provisions

Their related sections and articles are listed in Appendix A.

3.6 The Portal, Virtual Network and Sustainability of Results

In parallel with the main activities for developing and launching the ESCWA Cyber Legislation Directives, ESCWA had another aim for disseminating and supporting these efforts. This was carried out through two related processes:

1. Making available information about the Harmonization Project including documents, studies, reports and related resources through the **ESCWA Cyber Legislation Portal**.

2. Developing a **virtual network**. This is essentially a portal whose aim is to support the cyber legislation environment in the Arab region, as a forum of discussion and database of experts and institutions. The virtual network also aims at providing continuity of operations in the field of cyber legislation in the Arab region. It is the first portal of its kind in the region.

Most of the documents referred to in this digest are linked in the footnote to ESCWA's cyber legislation portal.

This section will concentrate on the virtual network as a part of the Harmonization Project.

Objectives of the Virtual Network

The main objectives of the virtual network are the following:

1. To support decision makers and legislators in Arab countries when developing legislation frameworks that cover cyberspace operations.

2. To ensure the streamlining of such frameworks regionally and through the use of the ESCWA cyber legislation directives.

3. To make available a platform that provides opportunities for cooperation and regional ongoing integration in the coordination of the cyber legislative process.

4. To make available a platform for the exchange of views and expertise.

5. To raise awareness of the importance of cyber legislation in the development of Knowledge-based economies and societies.

6. To assess and evaluate the current status of cyber legislation in Arab countries and compare it with regional and international cyber legislation.

One of the direct objectives noted for the virtual network is the reinforcement of regional integration and the development of capacity for the countries in the region, in their efforts to develop legislative and regulatory frameworks.

Components of the Portal & Virtual Network

The virtual network contains the following key components:

1. The content of the portal contains scientifically organized and documented information on various issues of cyber legislation. Such as:

   - Cyber legislation texts based on national, regional and international sources;
   - Information covering the Harmonization Project and its activities;
   - Cyber legislation related conventions and agreements from the Arab world or other countries;
   - Studies and directives issued by ESCWA;
   - Cyber legislation related references and reports;
   - ESCWA template for cyber legislation;
   - Matrices showing the status of cyber legislation in selected countries of the Arab world.

2. The Interactive component which provides opportunities to cooperate in order to adapt and maintain cyber legislation in an up to date form. This will allow:

   - The exchange of knowledge and best practices as well as dialog between experts and stakeholders;
   - Highlighting of pending issues;
   - The sharing of documents, expertise and success stories;
   - Updating the portal with news, events and related activities;
   - Feedback from users aimed at improving the website.

3. A membership database that hosts the profiles of experts and professionals in the field of cyber legislation.

4 A database that hosts specific information related to ministries, organizations and other stakeholders.

5. An advanced search engine that allows the extraction and production of beneficial reports from the portal.

Users of the Virtual Network

The users of the virtual network consist of two categories:

1. Experts and professionals who will have special modes of registration, which would provide special facilities such as the use of interactive tools and the participation in web based discussions.

2. Regular users who can register and have access to browse the portal as well as download various documents, studies and reports.

3.7 Advisory Services Offered by ESCWA

Throughout the Harmonization Project, ESCWA offered advisory services to its member countries, notably the following:

1. Oman: review cyber laws, one on e-commerce and the other on e-communications.
2. Palestine: review selected cyber laws.
3. Syria: review of five draft cyber laws.
4. Bahrain: to develop a gap analysis study between Bahraini cyber laws and the ESCWA Cyber Legislation Directives.
5. Jordan: to review the e-Transactions and Privacy law.
6. Sudan: to arrange a national training workshop on the ESCWA Cyber Legislation Directives.
7. Lebanon: To arrange a national seminar on cyber legislation addressed to the parliament and lawyers.

4.0 Recommendations

The Harmonization Project has always looked forward to major upgrades. Recommendations were issued as a result of proposals from regional experts in cyber legislation, as well as recommendations from ESCWA meetings and workshops.

4.1 Government Level Recommendations

The following recommendations were issued for local implementation:

1. To highlight the importance of covering comprehensive cyber legislation.
2. To stress the importance of acquiring guidance from, as well as joining, international cyber legislation agreements and those issued in the Arab region.
3. To urge governments to proceed with the implementation of cyber legislation.
4. To ensure that within each country, there is coordination between different governmental bodies to avoid duplication of legislation.
5. To avail the required human and financial resources for the ongoing fieldwork.

4.2 Regional Recommendations

The following recommendations apply at a regional level:

1. To stress the need for regional cooperation in matters related to cyber legislation by stressing the efforts made by the League of Arab States, ESCWA and regional and international organizations.
2. To highlight the importance of the ESCWA cyber legislation directives.
3. To draft an integrated agreement between Arab countries, that covers the six directives developed by ESCWA.
4. To develop plans that will develop and implement cyber legislation.
5. To facilitate electronic exchange between the countries in this region and build Arabian information societies.
6. To work on the unification of Arabic ICT and cyber legislation terminology in coordination with the League of Arab States.
7. To develop a legal Arabic database thesaurus.

4.3 Capacity Building and Training Recommendations

The following recommendations are addressed at the capacity building and training level:

1. To train legislators, judges and lawyers on cyber legislation.

2. To organize national training workshops for judges, lawyers, technicians, members of the prosecution, security forces and judicial officers.

3. To stress the need to conduct regional meetings and conferences for experts in cyber legislation.

4. To prepare for the qualification of judicial officers and authorities.

5. To appoint prosecution and special courts specialized in cyber legislation.

6. To include subjects related to cyber legislation in the syllabuses of ICT colleges and universities.

4.4 Recommendations for the Legislative Processes

The following are recommendations made to cover the process of legislation in various countries:

1. To ensure that legislation emanates from civil society, making it more authentic, rather than import concepts and operations from outside the region. This can be achieved through:

    - Publishing the proposed Cyber Legislations;
    - Improving transparency in the legislation process;
    - Widening the pool of stakeholders for formulation of cyber legislation.

2. To encourage documentation of all discussions in legislative committees and teams.

3. To develop the competence needed for formulating clear legislative texts including official commentary on each of the articles.

4. To develop methods of observation and fieldwork in parallel with the legislative process.

5. To document and make possible the recall of jurisprudence. This can be achieved by conducting studies that rely on fieldwork, without restricting what may be published of court decisions and decisions that resolve conflicts in cyberspace.

6. To form groups specialized in cyberspace jurisprudence to help in publishing judgments and case commentaries.

7. To highlight the importance of preparing comparative analyses over jurisprudence related to cybercrime, issued in the Arab region and in developed countries.

4.5 Other Recommendations

ESCWA recommends the following additional steps in addition to those mentioned above:

1. To encourage non-governmental organizations (NGOs) working in the field of cyber legislation to form working groups, that can collectively lobby governments and legislative bodies to develop special laws related to cyber legislation.

2. To launch financial feasibility studies that identify the required financial resources for regulatory authorities and other bodies concerned with prosecution, penalization and control, as well as identifying the most suitable forms for funding such operations all with the aim of implementing effective laws.

3. To make available the means and financial and human resources needed for ongoing fieldwork for regulatory authorities. This would allow them to conduct registration, profiling and surveying of various cyberspace operations at the national level.

5.0 Process and Methodology

This section provides an overview of the process and methodology that ESCWA used throughout the development and implementation of the Cyber Legislation Initiative.

5.1 Activities

The activities initially planned for this project were the following:

1. To produce a report that will:

    a) Identify major areas of concern for ESCWA member countries.
    b) Update the status of cyber legislation in the Arab region.
    c) Propose a framework for the regional harmonization of cyber legislation in the Arab world.

2. To take into account past international experience (mainly the European Commission's) to produce a set of directives which:

    a) Comprise text models of cyber laws that may easily be implemented at the national level.
    b) Cover the six main areas of cyber legislation.
    c) Include a set of coherent definitions of all legal terms used.
    d) Include a detailed introductory statement of the fundamental purposes and guiding principles of the directives.

3. To organize an experts meeting, involving professionals from governmental entities, non-governmental organizations and the private sector to review the directives that were proposed for the enhancement and harmonization of cyber legislation in the Arab region.

4. To organize two regional workshops that will provide hands-on training, to policy and decision makers, on the ESCWA cyber legislation Directives and their applications at national and regional levels.

5. To provide advisory services to ESCWA member countries and, upon request, other Arab countries on the drafting of legislation that would be in harmony with the ESCWA cyber legislation directives.

6. To organize a seminar on the legal and regulatory requirements for a sustainable knowledge society in the Arab region, to review the results of the harmonization process at the regional and sub-regional levels and provide recommendations for sustainability.

7. To promote and assist in the establishment of a Virtual Network of governmental, private sector and NGO institutions concerned with the promotion of the ICT sector. This activity will improve the sustainability of the project by helping various

stakeholders interact and exchange knowledge during and after the implementation of the project.

5.2 Research

The research conducted by ESCWA encompassed the following areas:

- Reviewing the experiences and activities of international organisations such as the EU, ITU, etc.
- Reviewing the experiences and activities of Arab based organisations and ESCWA member countries.
- Information from various legislations issued by Western countries such as the USA, France, Belgium, Switzerland, etc.
- Reviewing key cyber related jurisprudential references in Arabic and other languages.
- Referencing ESCWA studies related to cyber legislation for specific member countries in particular.

5.3 The Different Approaches Considered

ESCWA considered the following three approaches to tackling the implementation of cyber legislation in its member countries and the Arab region.

The first approach was to draft a specific legal framework for each cyberspace issue.

The second approach was to modify existing and applicable laws (this approach would be applicable in some cases only). These laws could be adjusted through the addition of articles or sections that regularize laws relating to cyberspace.

The third approach was to draft unified and consolidated laws that cover the various issues in cyberspace, in such a manner as to create a single law categorized into classes of issues in cyberspace.

ESCWA eventually adopted the first approach after the re-categorization of the various issues under the six compatible directives.

5.4 The Six Directives: Consolidating Cyberspace Issues

ESCWA's initial research resulted in identifying a large number of cyberspace related facilities, activities, components and issues:

- Electronic transactions;
- E-Commerce;
- The protection of personal data;
- Cybercrime;
- Electronic communication;

- Freedom of expression via electronic communication;
- Protection of intellectual property;
- Rules of evidence and the bases for decision and rulings;
- Combating terrorism on the Internet – cyberterrorism;
- Net neutrality;
- ICT laws and regulations;
- Computer forensics;
- e-Government;
- Adjudication via the Internet;
- Ethical and professional controls in the Internet;
- The basis and control of cloud processing

The above areas were too numerous and would have created an obstacle to building consensus with a need for early implementation of cyber legislation. Therefore, ESCWA re-categorized the above items into six main directives for improved focus and ease of development. The final six directives are:

1. e-Communication and freedom of expression;
2. e-Signature and e-Transactions;
3. e-Commerce and consumer protection;
4. The processing and protection of personal data;
5. The prevention and judicial processing of cybercrime;
6. Intellectual Property Rights in ICT and cyberspace.

5.5 Stakeholders of the Cyber Legislation Harmonization Project

ESCWA is currently implementing this project in coordination with several regional and international organizations. The purpose is to develop cyber legislation which would include the League of Arab States, the North Africa Office of the Economic Commission for Africa (ECA-NA) and others. ESCWA is notably collaborating with high level experts, government ministries, and specialized partners such as national and regional ICT societies and lawyer syndicates.

Beneficiaries of the Project

Most parties in the ESCWA region or the Arab world will directly or indirectly benefit from the results of the Harmonization Project. However, to arrive at a practical working plan, ESCWA focused on the following beneficiaries:

- Decision makers concerned with cyber legislation.
- The ministries concerned with cyber legislation such as the ministries of justice, commerce, interior and telecommunications.
- Legislators, judges and lawyers.
- The private sector.
- Professional bodies and communities.
- Members of the civil society.

Partners in the Project

The following is a list of parties involved in the development of the Harmonization Project:

1. ESCWA's Information and Communication Technology Division (ICTD).
2. Experts in the field of cyber legislation from the Arab region.
3. The Steering Committee for the project (see below).
4. Various cyber legislation experts and consultants.

Steering Committee

The Steering Committee of the Harmonization Project was established in early 2009 to provide guidance and advice on the implementation of the project's different phases and components. Other functions covered the monitoring of progress and the evaluation of the project's achievements.

The Committee had its first meeting in December 2009 (see section 5.8). It consisted of the following parties:

1. ESCWA representatives from ICTD.
2. The Director of the Arab Regional Bureau, International Telecommunication Union (ITU).
3. The Regional Adviser on ICT Policy, the Economic Commission for Africa North Africa Office (ECA-NA).
4. The representative of the Legal Department of the League of Arab States.
5. The representative of the Arab Administrative Development Organization (ARADO).
6. A regional expert in cyber legislation and his team.

Legal and ICT Advisors and Consultants

Throughout its development, the ESCWA Harmonization Project depended, to a large extent, on the expertise and guidance of various legal and ICT advisors and consultants.

Their expertise and guidance were offered through one or more of these channels or roles:

- Members of the Steering Committee;
- Speakers in the various workshops and conferences;
- Writers of specific papers.;
- Consultants to assist in the development of various documents in the project;
- Participants in the Experts General Meetings;
- Reviewers of draft documents.

Appendix A: The Six Directives – Detailed Laws and Articles

Directive 1: e-Communication and Freedom of Expression

The following is a summary of the proposed legal framework:

Chapter 1: General Provisions

Article 1: Definitions of terms such as:

- Electronic and online data transfer to the public
- Network and Communications Service Providers
- Data Hosting Service Providers
- Data traffic information
- Storage of information
- Encryption tools
- Encryption of information

Article 2: Freedom of electronic data transfer to the public

Chapter 2: The Legal Framework for the Network Service Providers

Article 3: Constraining of access to specific websites and services

Article 4: Controlling the Communications Service Providers and Data Hosting Service Providers

Article 5: Notifications to providers regarding the illegality of information

Article 6: The confidentiality of the identity of disseminators of information and the protection of the data related to his/her identity

Article 7: The storage of information regarding data traffic

Article 8: The provision of data traffic information to security and judiciary authorities

Activity 9: The contribution of Communications Service Providers and Data Hosting Service Providers in the combating of cybercrime.

Activity 10: The contractual obligation of the Communications Service Providers and Data Hosting Service Providers

Activity 11: The rights of a person addressed through electronic data transfer to the public to respond

Chapter 3: Data Encryption

Article 12: The usage of encryption tools, their provision, import and export

Article 13: The responsibilities of the providers of encryption tools

Chapter 4: Electronic Surveillance on Private and Personal Communications

Article 14: The inadmissibility of electronic surveillance on private and personal communication

Article 15: The admissibility of electronic surveillance based on judiciary decree or when national security is at stake

Chapter 5: Criminal Provisions

Article 16: Criminal Provisions

Directive 2: e-Signature and e-Transactions

The following is a summary of the proposed legal framework:

Chapter 1: General Provisions

Article 1: Scope of implementation

Article 2: Definitions of terms such as:

- Electronic records
- Electronic signatures
- Advanced electronic signatures
- Signatories
- Authorized and relying parties
- Pre-requisite data to create and check e-signatures
- Tools for creating and checking secure e-signatures
- Qualified certificates
- e-Signature products
- Voluntary accreditation
- Electronic payments and transfers
- Banking cards for use to withdraw, transfer or withdraw funds
- Electronic money and checks

Article 3: Issues related to local markets

Chapter 2: Electronic Records and Signatures

Article 4: Secure tools for the creation of e-signatures

Article 5: Definition of "electronic writing" and records and their tracking

Article 6: Official and regular electronic records

Article 7: Official tracking of e-signatures

Article 8: Checking the correctness and authenticity of electronic records and signatures

Article 9: Storage of electronic records

Article 10: Electronic tracking and the related printed paper document of electronic records

Chapter 3: The responsibilities of Authentication Service Providers, the owner of the certificate and the relying party

Article 11: Authentication Service Providers

Article 12: The responsibilities of Authentication Service Providers

Article 13: The responsibilities of the owner of authenticated certificates

Article 14: The responsibilities of the Relying and Authorized parties

Chapter 4: Legal recognition of Authentication Certificates issued in Countries outside the Arab Region

Article 15: Legal recognition of Authentication Certificates issued in countries outside the Arab Region

Chapter 5: Banking and Financial Transactions

Article 16: The issue of e-payment and e-transfer orders
Article 17: Electronic systems for the issue of e-payment and e-transfer orders
Article 18: The responsibility of the client for e-payment and e-transfer orders
Article 19: The responsibility of banks and financial institutions for e-payment and e-transfer orders
Article 20: The modification of contractual terms
Article 21: The issue of banking cards
Article 22: The responsibility of banks and financial institutions as regards banking cards
Article 23: The responsibility of the owner of banking cards
Article 24: Electronic money
Article 25: Electronic checks
Article 26: Final Provisions

Directive 3: e-Commerce and Consumer Protection

The following is a summary of the proposed legal framework:

Chapter 1: General Provisions
Article 1: The objectives of the Directive and its scope of implementation
Article 2: Definitions of terms such as:

- Electronic commerce (e-Commerce)
- Electronic message
- The sender and receiver of the electronic message
- The intermediary
- Electronic services
- Electronic contracts
- The consumer
- The professional
- Commercial messages and communications
- Automated e-message system

Article 3: Freedom of e-Commerce

Chapter 2: Commercial Electronic Messages and Letters
Article 4: The attribution of electronic messages
Article 5: Acknowledgement of receipt of electronic messages
Article 6: Time and Place stamp for the sending and receipt of electronic messages
Article 7: The information required for commercial messages and communications sent/received electronically
Article 8: Spam (non-desired commercial messages and communications)
Article 9: Regulated professions

Chapter 3: Electronic Contracts
Article 10: The legal recognition of electronic contracts
Article 11: The use of automated e-message system in the drafting of electronic contracts
Article 12: The information required from the providers of services

Article 13: The setup of orders
Article 14: The fixing of prices
Article 15: The right to cancel and get refunded
Article 16: The operations related to the shipment of goods
Article 17: The responsibilities of the professional

Chapter 4: Final Provisions
Article 18: Codes of Conduct
Article 19: Dispute resolution
Article 20: Judicial recourses
Article 21: Cooperation between ESCWA member countries
Article 22: Consumer protection
Article 23: Sanctions

Directive 4: The Processing and Protection of Personal Data

The following is a summary of the proposed legal framework:

Chapter 1: General Provisions
Article 1: The subject of the Directive
Article 2: Definitions of terms such as:

- Personal data
- The processing of personal data
- Personal data records and files
- The processor of data
- The subject of the personal data
- Others: the natural or virtual parties other than the subject of personal data
- The receiver of data
- Approvals and permissions

Article 3: The scope of implementation for the Directive: the processing of data whose objective is national security or defense or activities related to criminal law as well as the processing by individuals of strictly personal data and for personal use.

Chapter 2: The Official Control Agency
Article 4: The setup of an independent official Control Agency whose mission is the control and supervision of the proper implementation of the laws of this Directive

Chapter 3: General Conditions for the Processing of Personal Data
Section 1: The Nature of Personal Data
Article 5: The processing of personal data through valid and secure operations

Section 2: The legality of processing personal data
Article 6: The terms for processing personal data

Article 27: Final Provisions

Directive 5: Cybercrime

The following is a summary of the proposed legal framework:

Chapter 1: Crimes whose target is Data
Article 1: The damaging of data: the illegal modification, removal, corruption and destruction of data
Article 2: Blocking data transfer

Chapter 2: Crimes whose target is Information Systems
Article 3: Illegal access to or camping in an Information Systems
Article 4: Illegal access to or camping in an Information Systems coupled with the damaging of data
Article 5: Hindering the operations of an Information System: Denial of Service (DoS), stoppages, disruption of operations, etc.

Chapter 3: Misuse of Information Systems and Software
Article 6: Misuse of Information Systems and Software

Chapter 4: Crimes of a Financial or Transactional Nature
Article 7: The use of Information Systems for fraud and deception
Article 8: The forgery of computer information
Article 9: The use of Information Systems for cyber embezzlement or theft of funds
Article 10: The use of Information Systems for unsolicited marketing or promotions
Article 11: Identity theft
Article 12: Viewing or disseminating secret or sensitive data

Chapter 5: Cybercrimes against Minors
Article 13: Definitions covering minors, pornographic media, sexual acts, etc.
Article 14: The production of pornographic material with the aim of dissemination through Information Systems
Article 15: The presentation of pornographic media to minor through Information Systems
Article 16: The dissemination of pornographic media to minors through Information Systems
Article 17: The procuring of pornographic media for use by minors through Information Systems for use by oneself or for another
Article 18: The possession of pornographic media for use by minors through Information Systems
Article 19: The encouragement or inciting of minors to commit illicit sexual acts
Article 20: Sexual harassment of minors through Information Systems

Chapter 6: Infringement of Intellectual Property Rights
Article 21: The use of a fraudulent author's name on a work
Article 22: Counterfeit of authorial signatures or stamps
Article 23: The copying or the piracy of digital products

Article 24: The sale or offer to sell or the distribution of a copied work
Article 25: Offences related to the infringement of copyright and related rights

Chapter 7: Crimes related to Banking Cards and Electronic Money
Article 26: Counterfeiting a Banking Card
Article 27: The use of a counterfeit Banking Card
Article 28: The receipt of funds issued through a counterfeit Banking Card
Article 29: The counterfeiting of Electronic Money

Chapter 8: Crimes against Private Data
Article 30: The unauthorized processing of private data
Article 31: The illegal processing of private data
Article 32: The dissemination or distribution of private data
Article 33: The failure to respond to the subject concerned when requesting the correction or the viewing of his/her private data

Chapter 9: Racial Crimes or Crimes against Humanity
Article 34: The dissemination and distribution of racial information through Information Systems
Article 35: The threatening or the attack of persons based on their race, creed or color through Information Systems
Article 36: The dissemination of information through Information Systems whose purpose is to deny or distort genocidal activities or crimes against humanity
Article 37: The assistance or incitement through Information Systems to commit crimes against humanity

Chapter 10: Drug and Gambling related crimes
Article 38: The ownership and operation of gambling operations on the Internet
Article 39: The facilitation and encouragement of gambling operations on the Internet
Article 40: The promotion of alcoholic beverages to minors on the Internet
Article 41: The promotion of drugs (narcotics) on the Internet

Chapter 11: Cybercrimes against Public and National Security
Article 42: Disruption of governmental operations through the use of Information Systems
Article 43: Failure to report or the false reporting of cybercrimes
Article 44: The acquisition of classified data through Information Systems
Article 45: The tampering with judiciary evidence based in Information Systems
Article 46: The transmission of data that can threaten public and national security through Information Systems
Article 47: Cyber Terrorism
Article 48: Incitement to homicide through the use of Information Systems

Directive 6: Intellectual Property Rights in ICT and Cyberspace

The following is a summary of the proposed legal framework:

Chapter 1: General Provisions

Article 1: Definitions of terms such as:

- Semiconducting products
- Topographies of semiconducting products
- Commercial investments
- Domain names
- Country Code top level domains (ccTLDs)

Chapter 2: The Legal Protection of Software

Article 2: The protection of software based on the rights of the developer
Article 3: The developers of Software
Article 4: The beneficiaries of legal protection based on Software as intellectual property
Article 5: The rights of Developers of Software
Article 6: Exceptions (or Exemptions) for the protection of the rights of Developers of Software
Article 7: Reverse engineering of software products
Article 8: Special measures for the protection of Software
Article 9: Relation of articles under Chapter 2 to other laws and regulations

Chapter 3: The Legal Protection of Databases

Section 1: The Scope of Application

Article 10: The scope of application of Chapter 3

Section 2: The Legal Protection of Databases as Intellectual Property of the Developer

Article 11: The terms for the Protection of Databases as Intellectual Property of the Developer
Article 12: The Intellectual Property of the developer of databases
Article 13: The Exclusive rights of the developer of databases
Article 14: The Exceptions (or Exemptions) for the rights of the Developer of Databases

Section 3: Legal Protection based on Personal Rights

Article 15: The terms for the legal protection of databases as a personal right
Article 16: The rights of Database users and their obligations
Article 17: Exceptions (or Exemptions) for the rights of holders of personal rights
Article 18: Duration of protection of personal rights

Section 4: Final Provisions

Article 19: Penalization of acts that infringe on rights
Article 20: The imperative and mandatory nature of some Articles

Chapter 4: The Legal Protection of Semiconducting Products

Article 21: The terms for the protection of semiconducting products
Article 22: The holder of the rights for protection for semiconducting products
Article 23: Registration of topographies of semiconducting products and the making available of such material
Article 24: The essence of exclusive rights on topographies of semiconducting products
Article 25: The legal duration for exclusive rights

Appendix B: The Timeline of the Harmonization Project

The following sections summarize the various workshops and meetings conducted by ESCWA as part of the overall harmonization of cyber legislation activities. They cover the period from 2007 when the initial activities began until present.

5.6 2007 (December): Peer Consultation Meeting and the Template

In December 2007, ESCWA organized a get-together for regional legal experts in Amman. The meeting was entitled "**The Peer Consultation Meeting on Cyber Legislation in the ESCWA Region**".[8]

The objectives of the workshop were:

- To meet with cyber legislation experts and present the June 2007 study entitled "Models for Cyber Legislation in ESCWA member Countries" for their review and comments.
- To create a core network of experts and institutions that would be involved in the continuous development, improvement and implementation of cyber legislation in the ESCWA region.

The workshop was attended by representatives from Egypt, Iraq, Kuwait, Lebanon, Palestine, Syrian Arab Republic, The Kingdom of Bahrain, The Royal Kingdom of Jordan, the Sultanate of Oman, Yemen and ESCWA.

The meeting covered two other activities:

1. The presentation and discussion of a **template** that aimed at helping with the development of an implementation strategy for cyber legislation in the region. (This is discussed in section 3.4).

2. The presentation of two case studies by representatives from Syria and Bahrain where the template was implemented. These helped highlight the applicability of the template at the country level as well as the relevance of the study's guidelines and recommendations.

5.7 2008 (December): Workshop on Cyber Legislation and Templates

During **15-16 December 2008** in Beirut, Lebanon, ESCWA followed up with an event related to the meeting of regional experts. The meeting was entitled "**Workshop on Cyber Legislation and its Implementation in the ESCWA Region**"[9].

[8] http://www.escwa.un.org/information/meetingdetails.asp?referenceNum=651E
[9] http://www.escwa.un.org/information/meetingdetails.asp?referenceNum=891E

Around 18 participants from 10 ESCWA member countries attended this workshop. They were made up of legal consultants and researchers, judges and lawyers, ICT and cyberspace experts as well as representatives of ministries of communications, Justice and specialized non-governmental organizations were involved.

The workshop essentially presented the templates and their main objectives. It offered training on the uses and application of the cyber legislation templates. It also introduced their application in 2 member countries of ESCWA (Syria and the Kingdom of Bahrain).

The participants called for the harmonization of cyber legislation across the region in order to:

- Facilitate the movement of merchandise and data across borders.
- Encourage the creation and proliferation of an information society.
- Spread the benefits of copyright protection laws to signatory countries.

5.8 2009 (December): First Steering Committee Meeting

During December 2009, ESCWA organized the first meeting of the project's **Steering Committee**, which consisted of members from various regional and international organizations involved in the development of cyber legislation in the Arab region.

The objectives of the meeting were to confer about the strategic implications and directions related to the implementation of the activities of this project. They would then be able to select those that are most attuned with the goals of the project.

The overall recommendations of the meeting were to:

1. Highlight the importance of producing a set of directives for the harmonization of cyber legislation in Arab countries. This set should cover the six main areas of cyber legislation.
2. To make use of the European Union's experience in cyber legislation for the development of a set of directives, guidelines and the models for the harmonization of cyber legislation.
3. To utilize the cyber legislation results and benefit from the experience of regional and international initiatives by such organizations as: the International Telecommunications Union (ITU), the Economic Commission for Africa North Africa Office (ECA-NA) and the League of Arab States.

5.9 2011 (February): Expert Group Meeting

The "Expert Group Meeting (EGM) on the Regional Harmonization of Cyber Legislation"[10] took place on 16-17 February 2011 in Beirut, Lebanon.

[10] http://www.escwa.un.org/information/meetingdetails.asp?referenceNum=1427E

The main aim of the meeting was to promote the advantages of the Harmonization Project. The meeting became an open forum for participants and allowed them to review, discuss, evaluate and propose improvements to the six directives of cyber legislation.

The main topics that were discussed include:

- the overall objective of the project and its activities;
- the six directives of the Harmonization Project;
- the first draft of the general guidelines for the harmonization of cyber legislation at the regional level;
- the status of cyber legislation in the Arab region.

The outcomes of the meeting included:

- A set of recommendations for the improvement of the six directives for cyber legislation.
- A set of recommendations for the improvement of the guidelines for cyber legislation.
- The initial definition of a regional network of experts and institutions that specialize in the field of cyber legislation.
- Finalization of the directives, taking into account the points of view of the various experts.

5.10 2011 (September): Second Steering Committee Meeting

ESCWA organized a second Steering Committee meeting on the 13th of September 2011 at the ESCWA headquarters in Beirut.

During the meeting, participants proposed a number of collaboration tracks with their related organizations. The overall recommendations of the meeting were to:

1. Consider the ESCWA cyber legislation directives as a reference for lawyers and legislators.
2. Strengthen the collaboration between ESCWA and the League of Arab States.
3. Advocate the ESCWA cyber legislation directives at the highest political levels in the region, especially at the level of the Arab Telecommunication and Information Council of Ministers.
4. Organize specialized workshops to build cyber legislation capacity and the use of the directives.
5. Emphasize the importance of ESCWA's cooperation with international and regional organizations working in cyber legislation (the League of Arab States, the International Telecommunications Union (Arab Regional Bureau), the Economic Commission for Africa North Africa Office (ECA-NA) and the Arab Administrative Development Organization (ARADO)).
6. Develop new and adapted strategies to sustain efforts in developing cyber legislation in the Arab region.

5.11 2011 (September): First Workshop on ESCWA's Six Directives

ESCWA organized this workshop to disseminate and promote the six directives. The workshop took place at the ESCWA headquarters in Beirut, Lebanon on 13 to 15 September 2011.

The workshop was attended by representatives from Iraq, Lebanon, Morocco, Palestine, The Kingdom of Bahrain, The Royal Kingdom of Jordan, The Sudan, The Sultanate of Oman, Yemen and ESCWA.

Several papers were presented in the workshop by ESCWA staff and legal experts. These papers were mainly based on the six ESCWA cyber legislation directives[11].

The main recommendations which were agreed during the workshop included to:

1. Highlight the importance of the ESCWA cyber legislation directives.
2. Raise awareness of the directives and arrange specialized workshops on their use.
3. Reinforce the role of ESCWA in collaborating with regional and international organizations including the League of Arab States.
4. Maintain sustainability through the Project's future activities including the planned virtual network.
5. Officially and regionally launch the six directives targeting the highest level of decision makers.

5.12 2011: Various Conferences and Workshops

Several conferences and workshops took place in 2011 in which ESCWA presented its progress in cyber legislation and promoted the six directives:

1. The 5th International Conference on Theory and Practice of Electronic Governance (ICEGOV2011).
   Tallinn, Estonia during 26-28 September 2011.[12]
2. The Second Gulf Cooperation Council e-Government Awards and Conference.
   Kuwait, 13-15 November 2011.[13]
3. Arab Women Summit: Empowering Arab Women through ICT.
   Rabat, Morocco during 6-7 December 2011.[14]
4. The 5th Arab Conference for Industrial Information
   The Role of Information and Communication in the Transformation to a Knowledge-Based Society.

[11] http://www.escwa.un.org/information/meetingdetails.asp?referenceNum=1439E

[12] http://www.icegov2011.icegov.org/
[13] http://egcc-kw-award.info/default.aspx
[14] http://events.idc-cema.com/eng/events/48105-arab-women-summit/7-overview

Rabat, Morocco during 20-22 December 2011.[15]

5. A workshop in the Sultanate of Oman on Cyber Crime in 2012
6. A workshop with the Association of Arab Lawyers on ESCWA Cyber Legislation Directives in 2012
7. A thematic session on "Regional Integration through ICT and e-Governance in the ESCWA region" during the 6th International Conference on Theory and Practice on Electronic Governance (ICEGOV 2012).
   Albany, USA, 22-25 October 2012.

5.13 2012 (March): Second Workshop on Cyber Legislation

This workshop was conducted in Cairo during 14-15 March 2012[16]. The workshop was called '**Developing and Harmonizing Cyber Legislation in the Arab Region'**. It was conducted in coordination with the League of Arab States and was geared towards a legal audience.
The main topics included:

1. A description of the ESCWA Harmonization Project.
2. A brief look at the status of cyber legislation in the Arab region.
3. A detailed description of the ESCWA cyber legislation directives.
4. The application of the ESCWA cyber legislation directives at the national level.
5. The guidelines for the enhancement and harmonization of cyber legislation at the regional level.

The outcomes of the workshop provided:

1. The ability of Arab legislators to review and enhance their national cyber laws to cover all aspects of cyber legislation.
2. Increased awareness of the status of cyber legislation in the Arab region and the need for its continuous development.
3. Dissemination of the ESCWA cyber legislation directives.
4. Improved understanding of the importance of harmonizing cyber laws at the regional level.
5. A framework for improving cyber legislation in Arab countries.

Several papers were presented in the workshop by ESCWA staff and legal experts. These are available on the dedicated web page for the workshop (see meeting footnote at the beginning of this section).

[15] http://www.aidmo.org/aiinc5/
[16] http://www.escwa.un.org/information/meetingdetails.asp?referenceNum=1785E

5.14 2012 (December): Seminar on Legal and Regulatory Framework Cyber Legislation

Under the patronage of the Lebanese Minister of Telecommunications, ESCWA organized a Seminar on Legal and Regulatory Requirements for a Sustainable Knowledge Society in the Arab Region at the UN House in Beirut on 19 and 20 December 2012[17].

The seminar was attended by 47 participants from 14 Arab countries representing governments, particularly ministries of justice and ICT, academic institutions, the private sector and civil society. The seminar was also attended by participants representing the League of Arab States (LAS) and UN organizations.

The seminar's sessions addressed the accomplishments of ESCWA's project and its main outputs, notably the ESCWA Cyber Legislation Directives. It also discussed the "Regional Framework for the Application of the ESCWA Cyber Legislation Directives in the Arab Region" and agreed on its recommendations. The presentations also featured experiences of some member countries with the advisory services offered by ESCWA in the application of the Directives at the national level. The seminar also discussed a proposed regional framework for the application of the Directives in the Arab region. The seminar also included presentations via video conference by the United Nations Office on Drugs and Crime (UNODC) and the United Nations Conference on Trade and Development (UNCTAD) in addition to a presentation by the International Telecommunication Union's consultant who gave a lecture on the requirements for combating cybercrime and ITU's activities in this regard.

The last session of the seminar summarized the challenges of the legal and regulatory framework of the knowledge society in the Arab region and identifies the main areas that require development.

[17] http://www.escwa.un.org/information/meetingdetails.asp?referenceNum=2002E