

ECONOMIC AND SOCIAL COMMISSION FOR WESTERN ASIA (ESCWA)

**MODELS FOR CYBER LEGISLATION
IN ESCWA MEMBER COUNTRIES**

United Nations

Distr.
GENERAL
E/ESCWA/ICTD/2007/8
27 June 2007
ORIGINAL: ENGLISH

ECONOMIC AND SOCIAL COMMISSION FOR WESTERN ASIA (ESCWA)

**MODELS FOR CYBER LEGISLATION
IN ESCWA MEMBER COUNTRIES**

United Nations
New York, 2007

07-0320

Foreword

It is generally accepted that cyberspace in the Economic and Social Commission for Western Asia (ESCWA) region cannot flourish without a proactive, favourable environment for the use of the Internet by people in their various activities. Given the importance of cyber legislation to the development of a modern information society, active efforts by Governments, the private sector and non-governmental organizations are essential for the establishment of the enabling environment needed for the appropriate use of cyberspace. While extensive study and regional analysis have been done for other areas of the world, comparable material on that subject is not available for the ESCWA region. As such, policymakers are not well prepared to address those issues. In addition, the nascent nature of the information society in most ESCWA member countries requires legislative action in order to create an adequate enabling environment.

An important factor for achieving the enabling environment for that sector is crafting cyberspace laws and adopting directives in the legislative, organizational and management domains. Acknowledging the need for regional integration in cyberspace legislation is of great importance to facilitating electronic interactions between ESCWA member countries or at the Arab regional level. Certain parts of the world have already adopted directives at the regional level, including, as a prominent example, the European Union. This study provides an introduction to the topic and methodology of the research and contains a review of applicable cyber legislation at the international, regional and national levels. Moreover, it provides a foundation for the specific steps that can be taken by member countries, which are detailed in chapter 2, with recommendations, policy advice to enable member countries to assess their legal structures in those areas, and conclusions. The annexes of this study provide a quick reference for determining the status of cyber legislation in the region.

Mervat Tallawy
Executive Secretary of ESCWA

CONTENTS

Page

Foreword	iii
Introduction	1

Chapter

I. MODELS FOR CYBER LEGISLATION	3
A. Survey of legal texts	4
B. Cyber legislation in the ESCWA region	9
C. Analysis of current cyber or cyber-related legislation in the ESCWA region	14
II. RECOMMENDATIONS FOR DRAFTING A MODEL CYBER LAW IN THE ESCWA REGION	30
A. Mechanism for enacting cyber legislation	32
B. Conclusions	33

LIST OF BOXES

1. The main provisions of the Dubai International Financial Centre Authority Data Protection Law of 2007	17
2. Transfers of copies of works in electronic form in the United Kingdom	19
3. Country code top-level domain names (ccTLD)	23

ANNEXES

I. List of international and regional conventions	34
II. List of cyber legislation in the ESCWA region (in Arabic).....	36
III. List of cyber topics	39
IV. Comparative matrix of cyber legislation	42

Introduction

Technological development is an important economic issue for the ESCWA region. Countries with economies that are diversifying from their reliance on commodities, as well as developing countries, must pursue that issue proactively. Such issues as e-commerce and the development of a knowledge-based society depend heavily on technological enablers in order to develop properly.

To that end, there is a strong need for an appropriate legal foundation, generally referred to as cyber legislation. By definition, cyberspace is a virtual world that is wide and varied, one that encompasses such broad topics as personal data, electronic transactions, intellectual property and other related issues. That digital world, created by computers and communications tools, needs to be organized.

The term cyberspace has two meanings, namely: a broader term referring to the space related to the Internet, which is global and unattached to a geographical-jurisdictional scope; and a narrower meaning defined as a specified computer network or a database, either at a national level or relating to an Intranet or a local area network (LAN). An example of that is the computerization of the records pertaining to commercial registers, also known as registers of companies. In the ESCWA region, many countries are in the process of implementing similar computerization projects.

The Internet is difficult to regulate, given that no single legislature has jurisdiction to control an international domain. However, regulating national cyberspace is possible and often required. When cyberspace is left unregulated, users may hesitate to undertake transactions and dealings.

Legislation has always struggled to keep pace with the development of technology. Many Governments have created telecommunications rules and laws to protect and regulate computer data processing and handling. Local or, more specifically, national laws have had to be backed up with international conventions and agreements to avoid conflicts and to unify the efforts aimed at regulating and protecting computer networks and the interests of users.

E-commerce emerged with the use of the Internet, which brought to the fore new issues, namely, e-signature and certification of e-transactions. Procedural and judicial legal amendments or laws were instituted in order to allow both criminal and civil prosecution related to the misuse of computers and computer systems and networks.

Organizing and regulating cyberspace represents the first task, with main legal aspects being stipulated in parallel with such regulation. Subsequently, cyber crime can be combated in cases where offenders have infringed on intellectual property rights, or have obtained money or property through fraud or breach of security systems. Moreover, cyberspace can be regulated when countries enter into relevant conventions and agreements that stipulate the online dealings of the users of computer systems and the Internet.

In principle, the same crimes or acts considered illegal off-line are equally illegal and punishable under criminal and/or civil laws related to the online world. However, in cyberspace illegal acts and crimes take different forms with regard to the nature of the offender and the proof of the crime or the illegal act. Consequently, legislators have had to instigate new laws and regulations aimed at controlling the use of computer and computer-related data and transactions made in cyberspace. At the outset, the Internet was largely restricted to a specific target group, primarily military and intelligence, with correspondingly little need for laws and regulations. The early laws concerned mainly the protection of data and computer systems and focused mostly on protecting information from dissemination and illegal access, electronic wires and transfers and copyright.¹

¹ Within that context, the United Kingdom of Great Britain and Northern Ireland enacted the Computer Misuse Act of 1990, which replaced the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Strasbourg, 28 January 1981). Equally, the United States of America had introduced earlier legislation regulating computer use and related crimes, including computer fraud, wire fraud and copyright infringement.

This study combines cyber crimes of several kinds, namely: (a) criminal activity whereby computers or networks are an essential part or the target of crimes, including malicious code and defeating access control; and (b) traditional crimes that are facilitated by the use of computers or networks, including wire fraud, cyber-stalking, intellectual property infringements and content crimes.

Online crime grew with the evolution of the Internet, which in turn resulted in the need to organize and protect public use in order to maintain a secure space where data and intangible money could be stored, shared and transferred legally, and where personal data could be shared securely. Within that context, legal protection had to cover all possible legal issues and aspects, whether related to commerce, personal and human rights and procedural acts, with regard to the collection of evidence in electronic form, specifically electronic evidence and electronic signatures.

In view of all the above, there was a need to review international conventions and national laws that had adopted cyber legislation at the early stages in order to build up a comprehensive index showing the main topics to be regulated in order to secure cyberspace.

This study reviews the status of those local and international laws within the ESCWA region. In addition, specific examples of legislative principles help to illustrate the benefits and challenges of enacting more comprehensive cyber legislation. Such information can enable policymakers and legal professionals to determine legislative priorities for their jurisdictions. The study was created after an exhaustive review of cyber legislation at the international, regional and national levels. It analyses the following topics: (a) protection of individual and personal data; (b) protection of privacy and freedom of information in the electronic communications sector; (c) copyrights, neighbouring rights and industrial property rights within the information society; (d) electronic transactions; (e) e-commerce; and (f) cyber crimes.

I. MODELS FOR CYBER LEGISLATION

A review of national laws regulating the various legal aspects related to cyberspace, in addition to an analysis on the current status of relevant international conventions and agreements, revealed five main legal topics, namely: (a) data protection and processing, including privacy rights; (b) e-commerce; (c) e-transactions, including, for example, e-banking and e-payment; (d) cyber crime; and (e) intellectual property.

In the ESCWA region, the analysis revealed that, while cyber-related laws have been enacted in some countries, most still lack adequate and/or comprehensive cyber legislation. Within that context, the main topics for those member countries which have initiated such legislation relate to e-commerce, including e-signature, acceptance of e-documents and e-contracts; as well as to intellectual property issues, which are largely addressed under general copyright laws, rather than under specific cyber laws related to intellectual property.

This study analyses the status of cyber legislation of all the ESCWA members, namely: Bahrain, Egypt, Iraq, Jordan, Kuwait, Lebanon, Oman, Palestine, Qatar, Saudi Arabia, the Syrian Arab Republic, the United Arab Emirates and Yemen. A description of the current situation of cyber legislation in the ESCWA region is set forth below according to applicable national legislation in force, whether purely domestic or as decrees and regulations implementing international conventions and treaties related to cyberspace. This study highlights the absence of cyber legislation through a presentation of the legal topics and corresponding laws for each ESCWA member country.

The analysis is based on a comparison with the relevant cyber topics and legal frameworks stated in corresponding laws in Europe, the United States of America and Asia; and with the articles of various international conventions regulating cyber crimes and related legal issues, including security of e-transactions, e-commerce, procedural law and e-signature. At the outset, the analysis detects the presence or absence of cyber legislation in each member country and, subsequently, examines whether the existing legislation is adequate and sufficiently comprehensive. Moreover, it defines the necessary mechanism for a legislative body to study and enact a domestic cyber law in such specified subjects as e-trade, e-banking and compute crime protection.

In order to gather the required information and statistics for this study, research was undertaken on the available cyber-related conventions and treaties and on existing cyber laws in the United States of America, member countries of the European Union (EU), Canada and Australia. The research led to the establishment of an index detailing the topics of cyber-related legal issues as treated in international conventions and national laws.

This chapter comprises the following three sections:

(a) Survey of legal texts, including international conventions, directives and treaties; and national laws of selected countries. The summary highlights the main topics of each reviewed convention, agreement and national law based on the list of indexed topics;

(b) Cyber legislation in the ESCWA region, including full legal texts and articles of laws on such cyber-related topics as e-commerce, consumer protection, intellectual property and e-transactions. Additionally, ratifications made by ESCWA member countries to international conventions are outlined;

(c) Analysis of current cyber or cyber-related legislation in the ESCWA region in terms of whether such laws are exhaustive for all topics, compared to international conventions and foreign cyber laws.²

² A supplementary list of forthcoming legislation is not included, given that unpublished laws and drafts are undergoing major amendments.

A. SURVEY OF LEGAL TEXTS

This survey comprises two major sections, namely: (a) international conventions, agreements and legal texts, including directives; and (b) national cyber or cyber-related laws of selected countries outside the ESCWA region.³

1. *International conventions and agreements*⁴

The reviewed conventions and agreements are set forth below, categorized by subject and according to the cyber-related legislation.

(a) *Cyber crime and the protection of computer systems and network*

In the area of cyber crime, the major legal texts consist of the following:

- (i) Convention on Cybercrime, the Council of Europe Treaty No. 185 (Budapest, 23 November 2001): defines the main aspects and nature of cyber and computer crimes;
- (ii) Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems, Council of Europe Treaty No. 189 (Strasbourg, 28 January 2003): supplements the provisions of the Convention on Cybercrime regarding the criminalization of acts of a racist and xenophobic nature committed through computer systems.

(b) *Protection of personal data*

In the area of protection of personal data, the major legal texts consist of the following:

- (i) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe Treaty No. 108 (Strasbourg, 28 January 1981), along with Amendments adopted by the Committee of Ministers in Strasbourg on 15 June 1999: aims to secure in the territory of each party and for every individual, irrespective of nationality or residence, respect for rights and fundamental freedoms and, in particular, the right to privacy with regard to automatic processing of personal data;
- (ii) Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding Supervisory Authorities and Transborder Data Flows (Strasbourg, 8 November 2001);
- (iii) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data: obliges signatories to enact legislation concerning the automatic processing of personal data in order to protect the privacy of such personal data;
- (iv) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications): complements Directive 95/46/EC and harmonizes the provisions required to ensure an equivalent level of protection of fundamental rights and freedoms and, in particular, the right to privacy with respect to the processing of personal data in the electronic communications sector and to ensure the free movement of such data and of electronic communications equipment and services in the EU;

³ Section C presents an analysis of the current cyber or cyber-related legislation in the ESCWA region in terms of the affiliations and ratifications with regard to the conventions and treaties covered in section A.

⁴ For a complete list of international conventions and agreements, see annex I.

(c) *Electronic communications*

In the area of electronic communications, the major legal texts consist of the following:

- (i) Draft declaration on freedom of communication on the Internet (Strasbourg, 8 April 2002);
- (ii) Community-COST Concertation Agreement on a Concerted Action Project in the Field of Teleinformatics (COST project 11 bis, 1980);
- (iii) Guidelines for the Regulation of Computerized Personal Data Files, adopted by General Assembly resolution 45/95 of 14 December 1990;
- (iv) Bucharest Declaration on Combating Counterfeiting and Piracy (12 July 2006);
- (v) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications);
- (iv) Cooperation Agreement between the European Economic Community and the Kingdom of Sweden on the Interconnection of the Community Network for Data Transmission (Euronet) and the Swedish Data Network for Information-Retrieval Purposes (14 December 1981).

(d) *Computer programs*

In the area of computer programs, the major legal texts consist of the following:

- (i) Organisation for Economic Co-operation and Development (OECD) Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (25 July 2002);
- (ii) Directive 91/250/EEC of 14 May 1991 on the Legal Protection of Computer Programs;
- (iii) Council Resolution 96/C 376/01 of 21 November 1996 on new Policy Priorities regarding the Information Society;
- (iv) Council Framework Decision 2005/222/JHA of 24 February 2005 on Combating Attacks against Information Systems;
- (v) Interpol Information Technology (IT) Security and Crime Prevention Methods.

(e) *E-commerce*

In the area of e-commerce, the major legal texts consist of the following:

- (i) Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures;
- (ii) United Nations Commission on International Trade Law (UNCITRAL): Recommendation on the Legal Value of Computer Records (1985);
- (iii) United Nations Convention on the Use of Electronic Communications in International Contracts, adopted by the General Assembly on 23 November 2005;
- (iv) Community-COST Concertation Agreement on a Concerted Action Project in the Field of Teleinformatics (COST project 11 bis, 1980);

- (v) Treaty Establishing the European Community (Nice Consolidated Version, 1 January 1958) Part 3: Community Policies, Title XIV: Consumer Protection; articles 129a and 153.

(f) *Intellectual property*

In the area of intellectual property, the major legal texts consist of the following:

- (i) European Convention Relating to the Formalities Required for Patent Application (Paris, 11 December 1953);
- (ii) European Convention Relating to Questions on Copyright Law and Neighbouring Rights in the Framework of Transfrontier Broadcasting by Satellite (Strasbourg, 11 May 1994);
- (iii) Community-COST Concertation Agreement on a Concerted Action Project in the Field of Artificial Intelligence and Pattern Recognition (COST Project 13, 1985);
- (iv) World Intellectual Property Organization (WIPO) Convention for the Protection of Producers of Phonograms Against an Unauthorized Duplication of Their Phonograms (29 October 1971);
- (v) WIPO Copyright Treaty (WCT), adopted in Geneva on 20 December 1996;
- (vi) WIPO Performances and Phonograms Treaty (WPPT), adopted in Geneva on 20 December 1996;
- (vii) International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations (Rome Convention 1961);
- (viii) Berne Convention for the Protection of Literary and Artistic Works, Paris Act of 24 July 1971 and amended on 28 September 1979.

2. *National cyber or cyber-related laws of selected countries outside the ESCWA region*

Title
Belgium
Loi visant à transposer certaines dispositions de la directive services financiers à distance et de la directive vie privée et communications électroniques
Loi transposant en droit belge la Directive européenne 2001/29/CE du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information
La nouvelle loi belge sur le commerce électronique
Loi modifiant le Code de la taxe sur la valeur ajoutée (facture électronique)
Loi sur certains aspects juridiques des services de la société de l'information
Arrêté royal visant à réglementer l'envoi de publicités par courrier électronique
Loi relative aux opérations effectuées au moyen d'instruments de transfert électronique de fonds
Projet de loi fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification
Arrêté royal organisant le contrôle et l'accréditation des prestataires de service de certification qui délivrent des certificats qualifiés
Signature électronique et les services de certification
France
Loi n° 2006-961 du 1 ^{er} août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information
Décret n° 2005-1450 du 25 novembre 2005 relatif à la commercialisation à distance de services financiers auprès des consommateurs

Title
Loi du 21 Juin 2004 pour la confiance dans l'économie numérique
Arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation
Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
Règlement n° 2002-13 relatif à la monnaie électronique et aux établissements de monnaie électronique
Loi n° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
Code Pénal Articles 226-16 à 24
Luxemburg
Règlement grand-ducal du 1er juin 2001 relatif aux signatures électroniques, au paiement électronique et à la création du Comité "commerce électronique"
Germany
Federal Data Protection Act of 20 December 1990 (BGBl.I 1990 S.2954), amended by law of 14 September 1994 (BGBl. I S. 2325)
Sweden
Personal Data Act (1998:204) of 29 April 1998
Switzerland
Ordonnance sur la conduite de la guerre électronique
Loi Fédérale sur les services de certification dans le domaine de la signature électronique No. 943.03
Swiss Informatics Society Code of Ethics
Romania
Anti-Corruption Law Title III on Preventing and Fighting Cyber Crime
Canada
Electronic Information and Documents Act, 2000 (Saskatchewan)
Some computer-related offences found in the 1998 Criminal Code of Canada
Personal Information Protection and Electronic Documents Act, 2000
Electronic Commerce Act (Newfoundland)
Electronic Transactions Act (Manitoba)
Electronic Transactions Act (Alberta)
Electronic Commerce Act (Yukon)
Electronic Commerce Act (Prince Edward Island)
Electronic Commerce Act (Ontario)
Electronic Commerce Act (Nova Scotia)
United States of America
Computer Security Act of 1987
Uniform Electronic Transactions Act
The Privacy Act of 1974 5 U.S.C. 552a
Electronic Signatures in Global and National Commerce Act (E-SIGN), at 15 U.S.C. 7001
United States Code Annotated Title 18: Crimes and Criminal Procedure Part I - Crimes, Chapter 47: Fraud and False Statements 1029. Fraud and related activity in connection with access devices
United States Code Annotated Title 18: Crimes and Criminal Procedure Part I - Crimes, Chapter 47: Fraud and False Statements 1030. Fraud and related activity in connection with computers
United States Code Annotated Title 18: Crimes and Criminal Procedure Part I - Crimes, Chapter 65: Malicious Mischief 1362. Communication lines, stations or systems
United States Code Annotated Title 18: Crimes and Criminal Procedure Part I - Crimes, Chapter 119: Wire and Electronic Communications Interception and Interception of Oral Communications 2510. Definitions

Title
United States Code Annotated Title 18: Crimes and Criminal Procedure Part I - Crimes, Chapter 121: Stored Wire and Electronic Communications and Transactional Records Access 2701. Unlawful access to stored communications
United States Code Annotated Title 18: Crimes and Criminal Procedure Part II - Criminal Procedure, Chapter 206: Pen Registers and Trap and Trace Devices Provisions of Section 225 ("Cyber Security Enhancement Act") of the Homeland Security Act of 2002, amending Title 18 of the United States Code Field guidance on new authorities that relate to computer crime and electronic evidence enacted in the United States Patriot Act of 2001
No Electronic Theft ("NET") Act
Anticybersquatting Consumer Protection Act
Act to regulate interstate commerce by imposing limitations and penalties on the transmission of unsolicited commercial electronic mail via the Internet
United Kingdom of Great Britain and Northern Ireland
Data Protection Act 1998
Computer Misuse Act 1990
Electronic Communications Act 2000
European Union
Council Resolution of 15 July 1974 on the Community Policy on Data Processing
Recommendation No R (85) 10 adopted on 28 June 1985 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications
Recommendation No (87) 15 adopted on 17 September 1987 concerning the regulating of the use of personal data in the police sector
Commission Recommendation 87/598/EEC of 8 December 1987 concerning a European code of conduct relating to electronic payments [Official Journal L 365 of 24.12.1987]
Recommendation No (88) 2 on piracy in the field of copyright and neighbouring rights adopted on 18 January 1988
Recommendation No (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes adopted on 13 September 1989
Council Decision 92/242/EEC of 31 March 1992 in the Field of Information Security
European Commission Green Paper of 27 July 1995 on Copyright and Related Rights in the Information Society [COM(95) 382 final – not published in the Official Journal]
European Parliament and Council Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data [Official Journal L 281 of 23 November 1995]
Recommendation No (95) 13 adopted on 11 September 1995 concerning problems of criminal procedural law connected with information technology
Council Resolution of 21 November 1996 on New Policy-Priorities Regarding the Information Society (96/C 376/01)
Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases
Commission Communication of 18 April 1997: A European Initiative in the Sector of Electronic Commerce
Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the Protection of Consumers in Respect of Distance Contracts
Commission Recommendation 97/489/EC of 30 July 1997 on Transactions by Electronic Payment Instruments and in Particular the Relationship Between Issuer and Holder
Directive 97/55/EC of the European Parliament and of the Council of 6 October 1997 amending Directive 84/450/EEC concerning Misleading Advertising so as to Include Comparative Advertising
Directive 97/66/EC on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector

Title
Communication from the Commission of 11 April 2000 to the Council and the European Parliament, entitled "The Organization and Management of the Internet", International and European Policy Issues 1998-2000 [COM(2000) 202 final - not published in the Official Journal]
Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 Laying Down a Procedure for the Provision of Information in the Field of Technical Standards and Regulations
Directive 1999/93/EC on a Community framework for electronic signatures
Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (Directive on Electronic Commerce)
Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the Harmonization of Certain Aspects of Copyright and Related Rights in the Information Society
Regulation (CE) No 45/2001 of the European Parliament and of the Council of 18 December 2001 on the Protection of Individuals with regard to the Processing of Personal Data by the Institutions and Bodies of the Community and on the Free Movement of Such Data
The Electronic Commerce (EC Directive) Regulations 2002 of 30 July 2002
Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications)
Communication from the Commission of 22 January 2004 on Unsolicited Commercial Communications or "spam" [COM(2004) 28 final – not published in the Official Journal]
Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency
Council Framework Decision 2005/222/JHA of 24 February 2005 on Attacks Against Information Systems
Decision No 854/2005/EC of the European Parliament and of the Council of 11 May 2005 Establishing a Multiannual Community Programme on Promoting Safer Use of the Internet and New Online Technologies
Communication from the Commission of 31 May 2006: A Strategy for a Secure Information Society – Dialogue, Partnership and Empowerment [COM(2006) 251 final – not published in the Official Journal]
United Nations entities
56/80 Model Law on Electronic Signatures adopted by UNCITRAL
51/162 Model Law on Electronic Commerce adopted by UNCITRAL
United Nations Manual on the Prevention and Control of Computer-Related Crime
Xxx Ref see note to author division Recommendation of the UN 15th conference - criminal law related to computer crimes (Rio de Janeiro, Brazil, 4-9 October 1994)
Model Law on Electronic Commerce with Guide to Enactment adopted by UNCITRAL
Global
IT Security and Crime Prevention Methods
Association of South East Asian Nations (ASEAN)
Malaysia
Computer Crimes Act 1997
Digital Signature Regulations 1998
Singapore
Electronic Transactions Act 1998

B. CYBER LEGISLATION IN THE ESCWA REGION

The translations of the Arabic legal texts set forth below are for the purpose of this study and are not to be considered official translations (see annex II for the Arabic version of these texts).

1. Bahrain

In Bahrain, the major legal texts consist of the following:

- (a) E-Commerce Law of 14 September 2002 and the amendments of article 21 thereof by Law No. 13 of 2006;
- (b) Decree No. 9 of 12 January 2003 on the creation of a central data centre;
- (c) Decree No. 28 of 2002 on electronic transactions;
- (d) Law of Telecommunications No. 48 of 2002;
- (e) Executive Decision No. 25 of 9 July 2005 on the establishment and formation of the Higher Committee for Information Technology and Telecommunications;
- (f) Ministerial Decision No. 2 of 19 June 2006 on technical aspects accepted by official bodies for electronic transactions;
- (g) Decision No. 3 of 21 January 2001 concerning the formation of a committee regulating the e-commerce;
- (h) Law No. 22 of 25 June 2006 on copyright and neighbouring rights, whose implementing regulations have not yet been issued, annulled the Copyright Law No. 10 of 1993.

2. Egypt

In Egypt, the major legal texts consist of the following:

- (a) E-Signature Law of 21 April 2004;
- (b) Telecommunications Law No. 10 of 2003;
- (c) Law No. 82 of 2 June 2002 on intellectual property pertaining to trademarks, commercial data, geographical indications, patents of invention, utility models, layout designs of integrated circuits, undisclosed information, industrial designs and models, copyright and related rights and plant varieties. The implementing regulations related to copyright and related rights of the Law were issued as a ministerial decree on 14 April 2005;
- (d) Decree No. 327 of 2005 on establishing a division for the combating of computer and Internet crimes;

3. Iraq

In Iraq, cyber laws or amendments to existing laws concerning cyber-related legal aspects have not been enacted.

4. Jordan

In Jordan, the major legal texts consist of the following:

- (a) E-Transactions Law No. 85 of 2001;
- (b) Temporary law of 2003 on applying IT resources in government entities;
- (c) Copyright Law No. 22 of 1992 and its amendments of 1998, 1999 and 2005 governing the protection of copyright and related rights in Jordan.

5. Kuwait

In Kuwait, the major legal texts consist of a draft law on e-commerce, which is in the process of enactment; and Copyright Law No. 5 of 1999 on the protection of copyright for material published in all media.

6. Lebanon

(a) Intellectual property

In the area of intellectual property, the major legal texts consist of the following:

- (i) Artistic and Literary Ownership Law No. 75, enacted on 3 April 1999 and entered into force on 6 June 1999, governs copyright protection;
- (ii) Ministerial Directive No. 4 of 25 May 2006 on the protection of computer programs and combating piracy in Lebanon.

(b) Consumer protection

In the area of consumer protection, the draft law on consumer protection was established by Decree No. 13068 of 5 August 2004, which was approved as amended by the joint parliamentary committees and the Parliament.

(c) E-commerce (e-banking)

In the area of e-commerce (e-banking), the major legal texts consist of the following:

- (i) Monetary and Credit Law of 1 August 1963, articles 33, 70, 80 and 174;
- (ii) Law No. 133 of 26 October 1999 appointing the Central Bank regulator for credit cards and e-transactions. The enacted regulations concerning e-transactions are applicable through a decision issued on 30 March 2000 by the Central Bank;
- (iii) Circulars issued by the Central Bank concerning e-payments and use of magnetic cards are as follows: (a) "Electronic banking" of 23 December 2005; (b) "Electronic banking and financial transactions" of 3 July 2003; (c) "ATMs and credit cards" of 26 August 2002; (d) "Electronic clearing house for credit cards and payment cards and debit cards issued in the Lebanese market and used on ATMs" of 24 January 2003; and (e) "List of credit cards used in Lebanon" of 7 November 2002.

(d) Money laundering

In the area of combating money laundering, the major legal texts consist of the following:

- (i) Law No. 318 of 20 April 2001 (Combating Money Laundering);
- (ii) Circular No. 7818 of 18 May 2001 concerning the supervision of banking and financial operations in order to combat money laundering;
- (iii) Circular No. 7299 of 10 June 1999 concerning ATM and payment cards (debit and credit);
- (iv) Procedure amendments to civil and criminal procedure codes to comply with e-commerce and cyber crime prevention and prosecution needs.⁵

⁵ Within that context, appointed police units are entitled to requisition computers while investigating cyber crimes.

(e) *E-commerce and e-transactions*

In the area of e-commerce and e-transactions, a new draft law was tendered to the Legislative Committee of the Parliament and a study thereof is still underway.⁶

7. *Oman*

In Oman, the major legal texts consist of the following:

- (a) Sultanate Decree No. 72 on money laundering, articles 2 and 5 thereof;
- (b) The Copyright Law, issued by Royal Decree No.37/2000 of 21 May 2000, became effective on 3 June 2000.

8. *Palestine*

In Palestine, the major legal texts consist of the following:

- (a) Draft law concerning the country code top-level domain name (ccTLD) for Palestine, namely, “.ps” that will soon be enacted;
- (b) Civil and Commercial Procedure Law No. 4 of 2001, including article 19 thereof on the proof of e-signature;
- (c) Law No. 12 of 2004 on financial securities and article 26 thereof on e-signatures having the same validity as written signatures;
- (d) Executive Decision No. 35 of 2004 by the Council of Ministers on accessing the Internet through a Government computer centre;
- (e) Executive Decision No. 39 of 2004 by the Council of Ministers and annexed to Arbitration Law No. 3 of 2000, including article 19 thereof on the validity of contracts executed through electronic mail;
- (f) Executive Decision No. 74 of 2005 by the Council of Ministers on a national strategy for telecommunications and information technology;
- (g) Executive Decision No. 269 of 2005 by the Council of Ministers on general policies of the use on the computer and Internet in official institutions;
- (h) Executive Decision No. 65 of 2005 by the Council of Ministers on the adoption of the E-Palestine Initiative.

9. *Qatar*

In Qatar, the major legal texts consist of the following:

- (a) Draft law on cyber crime to be enacted soon;
- (b) Telecommunications Law No. 34 of 2006;
- (c) Copyright Law No. 25 of 22 July and published in the Official Gazette No. 14 of 12 August 1995. The implementing regulations have not yet been issued, thereby delaying the implementation of the Law.

⁶ The law is expected to be passed during 2006-2007.

10. *Saudi Arabia*

In Saudi Arabia, the major legal texts consist of the following:

- (a) Telecommunications Law of 2001;
- (b) Completed draft laws on e-transactions and cyber crimes, expected to be enacted in the near term;
- (c) Ministerial Decision No. 6667 concerning the conditions for practising IT and telecommunications counselling;
- (d) Copyright Law issued as per the Royal Decree No. M/41 of 30 August 2003 and published in the Official Gazette No. 3959 of 19 September 2003. The implementing regulations of the Law were published in the Official Gazette of 4 June 2004 and entered into force on 2 August 2004.

11. *Syrian Arab Republic*

Cyber laws or amendments to existing laws concerning cyber-related legal aspects have not been enacted in the Syrian Arab Republic. However, a draft law on e-signature has been presented to the Council of Ministers for adoption.

Copyright protection in the Syrian Arab Republic is governed by Law No. 12 of 2001. While the Syrian Copyright Protection Department (CPD) has started to process copyright applications, official fees have yet to be set.

12. *United Arab Emirates*

In the United Arab Emirates, the major legal texts consist of the following:

- (a) Federal Law No. 2 of 2006 on combating information technology crimes;
- (b) Law No. 2 of 2002 on e-commerce and e-transactions (Dubai);
- (c) Free Zone Law of Technology, E-Commerce and Information of 2000 (Dubai);
- (d) Customs Law of 1998, including articles 4, 24 and 118 on the validity of documents and information received electronically;
- (e) Law No. 1 of 2007, issued by the Dubai International Financial Center (DIFC), and Data Protection Law 2001, which is applicable in the jurisdiction of DIFC;
- (f) Copyright and Authorship Protection Law No. 7 of 2002.

13. *Yemen*

In Yemen, the major legal texts consist of the following:

- (a) Law No. 40 of 28 December 2006 concerning e-payment, e-banking and financial operations, e-contract and e-signature;
- (b) Press Law No. 20 of 1991;
- (c) Law No. 19 of 1994 on intellectual property rights (IPRs) whose stipulated protection for copyright has been delayed by the non-issuance of the implementing regulations.

C. ANALYSIS OF CURRENT CYBER OR CYBER-RELATED LEGISLATION IN THE ESCWA REGION

Generally, cyber or cyber-related legislation in the ESCWA region is either rudimentary or incomplete. There are wide disparities between the countries of the ESCWA region concerning the enactment of cyber laws. Specifically, while some countries, including Bahrain and the United Arab Emirates, have already introduced several cyber laws, others are still at the stage of reviewing drafts or drawing up legal texts.

However, most ESCWA member countries have acknowledged the importance of regulating cyberspace and the use of computer systems and the Internet. This fact can be ascertained by various e-government and draft legislation efforts undertaken across the region.

The comparison of international conventions, treaties and foreign local cyber or cyber-related laws with those enacted in the ESCWA region revealed a number of issues that are set forth below.

1. *Data protection and privacy rights*

Inadequate or non-existent disclosure control mechanisms represent the main cause for privacy problems, particularly because uniquely identifiable data related to a person or persons can be collected and stored in a digital format. Generally, the main types of data affected by data privacy issues relate to the following: health information, criminal justice, financial information, genetic information and location information.

The legal protection of the right to privacy in general, and of data privacy in particular, varies greatly across the world.

Article 12 of the Universal Declaration of Human Rights states that “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks”.⁷

The protection of privacy rights has necessitated that personal data stored or transferred using a computer or computer systems and networks must be regulated and protected through legal texts and directives.

At the international level, several conventions and directives have been promulgated and ratified by many countries in order to protect personal data, thereby protecting privacy rights. For example, EU has enacted conventions and directives that are applicable in its member countries and whose contents are included in their local laws. Within the framework of those directives and legal texts, EU addressed various issues, including the quality of the data to be processed and the criteria for making data processing legitimate, and the protection of such data against illegal disclosure or dissemination. Prominent among those directives and conventions are the following: (a) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications); and (b) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data.

The United States of America has a different perspective with regard to privacy rights, given that the regulation thereof sometimes contradicts the First Amendment on freedom of speech. Federal laws, including the Privacy Act of 1974, stipulate the conditions for the disclosure of records and the access thereto.

In order to comply with European regulations on data protection and privacy rights, the Department of Commerce in the United States has provided for a “safe harbor arrangement” whereby United States companies are compelled to comply with EU Directive 95/46/EC on the protection of personal data when dealing with their European counterparts.

⁷ The Universal Declaration of Human Rights is available at: www.un.org/Overview/rights.html.

Moreover, EU member countries have integrated the main principles for the protection and processing of personal data in their local laws. In addition, some EU regulations stipulate the protection of individuals with regard to the processing of personal data by EU institutions and bodies and on the free movement of such data.

In the United Kingdom of Great Britain and Northern Ireland, for example, the Data Protection Act of 1998 stipulates eight principles that are mandatory to the processing of personal data. According to the Protection Act, data must be fairly and lawfully processed; processed for limited purposes; adequate, relevant and not excessive; accurate; not kept longer than necessary; processed in accordance with the rights of the data subject; secure; and not transferred to countries without adequate protection.

The same principles were adopted in France under Law No. 78 of 17 January 1978 concerning freedom and data protection.⁸ Additionally, the Penal Code in France stipulates penalties for offences and infractions made against personal data, including imprisonment for up to five years and fines reaching 300,000 euros. The Penal Code also criminalizes offences caused by negligence or failing to apply to the measures for adequate protection or processing of data.

Similarly, Sweden issued the Personal Data Act (1998:204) on 29 April 1998, which fully complies with the principles for data protection and processing as set by EU Directive 95/46/EC on the protection of personal data.

Consequently, the international protection for data processing in automatic or semi-automatic systems follows the principles established by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe Treaty No. 108 (Strasbourg, 28 January 1981), by which the quality of the data to be automatically processed must have the following attributes: “(a) be obtained and processed fairly and lawfully; (b) be stored for specified and legitimate purposes and not used in a way incompatible with those purposes; (c) be adequate, relevant and not excessive in relation to the purposes for which they are stored; (d) be accurate and, where necessary, kept up to date; (e) be preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored”.

In the Arab region in general, and in the ESCWA region in particular, there is still an absence of specific and adequate laws protecting data processing and privacy rights. While some articles exist in national laws, these relate mainly to civil status, statistics or storing banking information. Data protection legislation is still lacking in many countries of the ESCWA region. In Tunisia, by contrast, chapter 6 of the E-Commerce and E-Transactions Law includes provisions to protect personal data. Other North African Arab countries, including Algeria and Morocco, have also applicable laws relating to the protection of data.

Against that background, the status of ESCWA member countries is summarized below.

(a) *Bahrain*: Existing cyber laws are silent on data protection and processing, and there is no evidence of a new draft being prepared or studied;

(b) *Egypt*: Article 2 of the Telecommunications Law No. 10 of 2003 defines the telecommunications service based on such principles as data being made public and rights of users being safeguarded. There is no evidence of other legislation concerning the protection or the processing of data;

(c) *Iraq*: There is no evidence of legal provisions concerning data protection or processing;

(d) *Jordan*: The E-Transactions Law is silent on data protection. While the temporary Law of 2003 concerns applying IT resources in Government entities, it is similarly silent regarding data protection. There is no evidence of a new draft being prepared or studied;

(e) *Kuwait*: There is no evidence of any legal provisions concerning data protection or processing;

⁸ This Law has been amended intermittently and the latest amendment was ratified in January 2006.

(f) *Lebanon*: There is no legislation concerning data protection and processing. While the draft law on e-commerce and e-transactions included a chapter dealing with the protection of data processing, it is now in Parliament pending further study and possible amendments prior to enactment;

(g) *Oman*: There is no evidence of applicable laws or provisions concerning data protection and processing, nor of legislation being prepared or studied;

(h) *Palestine*: There is no evidence of legal provisions concerning data protection or processing;

(i) *Qatar*: Existing cyber laws are silent on data protection. Article 35 of the earlier Telecommunications Law issued in 1987 defined the restrictions on receiving telecoms messages or signals not intended for the recipient or, if received unintentionally, the prohibition of keeping or disseminating such messages or signals. However, the new Telecommunications Law of 2006 Decree No. 34 represents a substantial progress in this field, stipulating, in articles 50 and 52, restrictions concerning consumer protection and data protection. Moreover, article 50 prohibits service providers from using consumer information to make unsolicited advertising; and article 52 prohibits service providers from breaching privacy rights of clients and to protect and safely store the collected client data.⁹ Article 52 is partially compliant with the provisions of EU Directive 95/46/EC on the protection of personal data regarding the principles of processing and protecting data. The search did not reveal a new draft being prepared or studied;

(j) *Saudi Arabia*: There is no evidence of legal provisions concerning data protection or processing;

(k) *Syrian Arab Republic*: There is no evidence of legal provisions concerning data protection or processing;

(l) *United Arab Emirates*: The Data Protection Law of January 2007 applies in the jurisdiction of the Dubai International Financial Centre (DIFC) and articles 8 and 10 thereof protect the processing of personal and sensitive data in line with EU and OECD directives. The Law specifies personal data as any information relating to an identifiable natural person; and sensitive personal data as revealing or concerning, directly or indirectly, racial or ethnic origin, communal original, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life;

(m) *Yemen*: There is no evidence of legal provisions concerning data protection or processing.

**Box 1. The main provisions of the Dubai International Financial Centre Authority
Data Protection Law of 2007**

General requirements

Data Controllers must ensure that the Personal Data that they Process is:

- Processed fairly, lawfully and securely;
- Processed for specified, explicit and legitimate purposes in accordance with the Data Subject's rights and not further Processed in a way incompatible with those purposes or rights;
- Adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed;
- Accurate and, where necessary, kept up to date; and
- Kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data was collected or for which they are further Processed.

⁹ Additionally, article 52 prohibits the service provider from collecting, saving, using or disseminating any data unless with approval from the client or as stipulated by the Law. The service provider is also responsible for ensuring that the data collected are true, complete and valid for use according to their purpose. However, official bodies have the legal right to obtain secret data or private communication.

Box 1 (continued)

Every reasonable step must be taken by Data Controllers to ensure that Personal Data which is inaccurate or incomplete, having regard to the purposes for which it was collected or for which it is further Processed, is erased or rectified.

Processing of sensitive personal data

Sensitive Personal Data shall not be Processed unless:

- The Data Subject has given his written consent to the Processing of that Sensitive Personal Data;
- Processing is necessary for the purposes of carrying out the obligations and specific rights of the Data Controller;
- Processing is necessary to protect the vital interests of the Data Subject or of another person where the Data Subject is physically or legally incapable of giving his consent;
- Processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body on condition that the Processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the Personal Data are not disclosed to a Third Party without the consent of the Data Subjects;
- The Processing relates to Personal Data which are manifestly made public by the Data Subject or is necessary for the establishment, exercise or defence of legal claims;
- Processing is necessary for compliance with any regulatory or legal obligation to which the Data Controller is subject;
- Processing is necessary to uphold the legitimate interests of the Data Controller recognised in the international financial markets, provided that such is pursued in accordance with international financial standards and except where such interests are overridden by compelling legitimate interests of the Data Subject relating to the Data Subject's particular situation;
- Processing is necessary to comply with any regulatory requirements, auditing, accounting, anti-money laundering or counter terrorist financing obligations or the prevention or detection of any crime that apply to a Data Controller;
- Processing is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those Personal Data is Processed by a health professional subject under national laws or regulations established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy;
- Processing is required for protecting members of the public against: (a) financial loss arising from dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment, management consultancy, IT services, accounting or other commercial activities (either in person or indirectly by means of outsourcing); (b) dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment, financial or other services;
- Authorized in writing by the Commissioner of Data Protection.

In subsequent articles, the Law stipulates the rules to follow when applying for data transfers outside the DIFC jurisdiction with adequate level of protection or with the absence of adequate levels of protection. Moreover, the Law provides, in part 3 thereof, the rights of Data Subjects to perform the following:

- To access and rectify, erase or block Personal Data;
- To object to processing.

The Law is considered complete in terms of protecting personal data and provides for safe use and processing regulations inside DIFC.

2. *Protection of privacy and freedom of information in the electronic communications sector*

Despite the consensus that the right to privacy is a fundamental one, it is not always respected online. Several countries have introduced legislation addressing the illegal collection, storage, modification, disclosure or dissemination of personal data, and interference in communications of private bodies and persons.

The countries of the ESCWA region lack adequate laws and regulations with regard to privacy and freedom of information. The only issue addressed is the protection of communication in various telecommunications laws across the region, including, for example, Egypt. Other provisions for the protection of privacy may be found in penal codes.

With the notable exception of the Data Protection Law of 2007 of Dubai in the United Arab Emirates, there is no evidence of any law that specifically mentions privacy protection online or in the electronic communications sector in the ESCWA region.

3. *Censorship and freedom of expression in cyberspace*

The freedom of expression and liberties in cyberspace, and more specifically on the Internet, represents another major topic that is subject to legal protection and regulation.¹⁰ Generally, Arab countries, including those in the ESCWA region, have severe censorship laws.

Another aspect of censorship relates to public morals, which are protected in the Arab countries in general. While the countries of the ESCWA region have not regulated freedom of speech and censorship on the Internet, they have addressed those issues in national laws, including those relating to media and information which regulate the press and television and radio broadcasting; and to the penal and criminal laws.

A brief summary of the status in some countries of the ESCWA region on censorship is set forth below:

(a) *Saudi Arabia*: The country directs all international Internet traffic through a proxy farm located in King Abdulaziz City for Science and Technology. Content filtering is implemented there, based on software by Secure Computing. Additionally, a number of sites are blocked according to two lists maintained by the Internet Services Unit (ISU), namely: (i) one containing “immoral”, mostly pornographic, sites;¹¹ and (ii) one based on directions from a security committee run by the Ministry of Interior. The legal basis for content filtering is a resolution by the Council of Ministers dated 12 February 2001;

(b) *United Arab Emirates*: The country censors the Internet using software by Secure Computing. The national Internet service provider (ISP), Etisalat, bans pornography, politically sensitive material, and any content deemed contrary to the moral values of the United Arab Emirates;

(c) *Yemen*: The two licensed ISPs block access to contents falling under the categories of gambling, adult content and sex education, as well as material seeking to convert Muslims to other religions.

In view of the above, and in contrast to countries in other regions which have enacted laws implementing the rules for protecting freedom of expression and the provisions of the United Nations Universal Declaration of Human Rights,¹² the countries in the ESCWA region still lack the adequate

¹⁰ In that sense, cyberspace refers to its broader definition (see p. 1).

¹¹ Within that context, citizens are encouraged to report “immoral” sites for blocking by using the Web form provided.

¹² Article 19 of the United Nations Universal Declaration of Human Rights, which was adopted in 1948, reads: “Everyone has the right to opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers”. Available at: www.un.org/Overview/rights.html.

regulation to ensure a censorship level that does not contradict internationally recognized rules on freedom of expression.

4. *Intellectual property*

The protection of IPRs in cyberspace is one of the most important legal issues on which numerous laws and international conventions and treaties have been adopted. That issue relates mainly to an infringement on the following IPRs or works: (a) computer programs and software, where the offences are generally categorized as either piracy and illegal copying, or unauthorized use and access; (b) domain names, through which copyright or trademark infringements can occur and where the offences are either piracy of copyrighted material and works, including, for example, downloading illegal copies of songs or movies, or enabling such access; (c) cyber-squatting, which is the infringement of a trademark over the Internet; and (d) cyber-smearing, which is the dilution of a trademark on the Internet.

In addition to the above, major IPRs can also be infringed using a computer or a computer system, including patents of software, whereby computer systems or reverse engineering methods are used to crack the algorithms of a particular piece of intellectual property.

Within that context, the main aspects of copyright infringements in cyberspace can be categorized as follows:

- (a) Downloads from and uploads to the Internet;
- (b) Databases, which can receive copyright protection for the selection and arrangement of content;

(c) Computer programs, whereby conversions of a program into or between computer languages and codes correspond to adapting a work; and storing any work in a computer amounts to copying that work. In addition, running a computer program or displaying work on a video display unit will usually involve copying and therefore require the consent of the copyright owner.

Box 2. Transfers of copies of works in electronic form in the United Kingdom

In the United Kingdom of Great Britain and Northern Ireland, article 56 of the Copyright, Designs and Patents Act of 1988 stipulates copyright protection regarding works in electronic form. The article applies where a copy of a work in electronic form has been purchased on terms which, expressly or implied or by virtue of any rule of law, allow the purchaser to copy the work, or to adapt it or make copies of an adaptation, in connection with his use of it.

Moreover, it applies if there are no express terms prohibiting the transfer of the copy by the purchaser, imposing obligations which continue after a transfer, prohibiting the assignment of any licence or terminating any licence on a transfer; or providing for the terms on which a transferee may do the things which the purchaser was permitted to do. Anything which the purchaser was allowed to do may also be done without infringement of copyright by a transferee; but any copy, adaptation or copy of an adaptation made by the purchaser which is not also transferred shall be treated as an infringing copy for all purposes after the transfer.

The same applies where the original purchased copy is no longer usable and what is transferred is a further copy used in its place. The above provisions also apply on a subsequent transfer.

In the ESCWA region, while national copyright laws do mention the protection granted for computer programs and databases, Internet or online copyright-related issues are not expressly defined. However, such infringements fall within the general meaning of the articles of the law, which signifies that the infringer of a copyrighted work online can be prosecuted under the copyright law.

The copyright laws of the ESCWA region are summarized and set forth below:

(a) *Bahrain*: Law No. 22 of 25 June 2006 relating to copyright and neighbouring rights governs the protection of copyright and related rights in Bahrain. The Law, whose implementing regulations have not yet been issued, annul the Copyright Law No. 10 of 1993.

Works protected under the new Law include: books, pamphlets and other writings; lectures and sermons; dramatic and cinematography works; musical works and compositions; works of drawing, painting, sculpture, engraving, applied art and architecture; photographic works; illustrations, maps and plans; sketches and three-dimensional works; and folklore expressions, as well as computer programs and databases if personally created. The Law also provides protection for neighbouring rights, including those of performers, producers of sound recordings and broadcasting organizations.

Infringements are prosecuted before the Civil Court of Bahrain, which can stop the circulation of infringing works, seize and destroy such works and the equipment used, estimate the illicit proceeds and call upon expert assessment. Under the new Law, penalties for copyright infringements have been stiffened to include imprisonment ranging between three months and one year and fines ranging between 500 and 4000 Bahrain dinars. Bahrain became a member of the Berne Convention for the Protection of Literary and Artistic Works on 2 March 1997;

(b) *Egypt*: Law No. 82 of 2 June 2002 pertaining to the protection of IPRs was issued to protect trademarks, commercial data, geographical indications, patents of invention, utility models, layout designs of integrated circuits, undisclosed information, industrial designs and models, copyright and related rights, and plant varieties.¹³

Original works of literature, art and science, regardless of type, importance or purpose, are protected. That includes works of art expressed in writing, sound, drawings, photography and cinematography, such as books, writings, speeches, oral works, plays, dramatic works, musical compositions, films, phonographic works, applied art, three-dimensional works, computer programs and national folklore. Such works are protected for the lifetime of the author plus 50 years following death. The Law also provides protection for related rights, including those of performers, producers of phonograms and broadcasting organizations.

The Law protects original works of art. The Supreme Council of Cultural Affairs at the Ministry of Culture reserves the right to allow the publication of a work of art for documentary, transitional, educational, cultural or scientific use under certain conditions. Law No. 82 abrogated Law No. 354 of 1954 pertaining to copyright protection.

Egypt became a member of the Berne Convention for the Protection of Literary and Artistic Works on 7 June 1977;

(c) *Iraq*: Order No. 83 issued by the Coalition Provisional Authority on 29 April 2004 amended Copyright Law No. 3 of 1971, which governed the protection of copyright in Iraq. However, the Order has still not been implemented. Protection is granted to every intellectual property, irrespective of type, method of expression, importance and purpose.

Works that can be copyrighted include written and oral works, computer programs, dramatic and musical works, cinematographic and photographic works, drawings and scientific three-dimensional figures. Protection for the lifetime of the author plus 50 years following death is granted. This protection extends to such related rights as those of performers, producers of phonograms and broadcasting organizations;

(d) *Jordan*: The Copyright Law No. 22 of 1992 and the amendments of 1998, 1999 and 2005 govern the protection of copyright and related rights in Jordan. Protection covers original works of literature, art and

¹³ The implementing regulations for article 3 relating to Copyright and Related Rights of Law No. 82 were issued as per ministerial decree on 14 April 2005.

science, regardless of type, importance or purpose, including works of art expressed in writing, sound, drawing, photography and cinematography, such as books, speeches, plays, musical compositions, films, applied art, three-dimensional works and computer software.

The duration of protection for copyrighted material is the lifetime of the author plus 50 years following death. The rights of performers and producers of phonograms are protected for 50 years, while the rights of broadcasting organizations are protected for 20 years.

The Ministry of Culture reserves the right to allow publication of the work of art if the copyright holder has not done so, or if the heirs do not publish it within six months of being informed to do so in writing. In that case, the Ministry of Culture will provide the copyright holder or the heirs with fair compensation. Infringements of the Law are prosecuted before the Civil Court of Jordan.

Jordan became a member of the Berne Convention for the Protection of Literary and Artistic Works on 28 July 1999;

(e) *Lebanon*: Copyright protection in Lebanon is governed by Artistic and Literary Ownership Law No. 75, which was enacted on 3 April 1999 and entered into force on 6 June 1999. The protection of that Law applies to every production of the human spirit, whether written, pictorial, sculptural, manuscript or oral, regardless of value, importance or purpose, and the mode or form of expression. That protection covers computer programs in any language.

The following derivative works are subject to the provisions of that Law and are protected as original works without prejudice to the rights in the original work: (i) any kind of plastic art work, whether intended for industry or not; (ii) translations, adaptations, transformations and arrangements of music; and (iii) collections of literary or artistic works and compilations of data, whether in machine-readable or other form, provided that they are authorized by the copyright holder or his public or private successors, and that, by reason of the selection and arrangement of content, they constitute intellectual creations.

Lebanon became a member of the Berne Convention for the Protection of Literary and Artistic Works on 30 September 1947 and of the Universal Copyright Convention on 17 July 1959;

(f) *Oman*: The Copyright Law, which was issued by Royal Decree No. 37/2000 of 21 May 2000, became effective on 3 June 2000. The Law grants protection to authors of literary, artistic and scientific works irrespective of value, kind, purpose or medium. Generally, protection is provided for the works whose means of expression is writing, sound, drawing, image or film, including creative titles and computer software, and which are published, acted or displayed for the first time in Oman or abroad.

The term of protection is the lifetime of the author plus 50 years following death. Copyrighted works can be deposited at the Ministry of Commerce and Industry and are considered a presumption of ownership.

Oman became a member of the Berne Convention for the Protection of Literary and Artistic Works on 14 July 1999;

(g) *Palestine*: There is no evidence of a copyright law in force;

(h) *Qatar*: While Law No. 7 of 2002 on the protection of copyright and neighbouring rights was issued, the implementing regulations have not yet been released, thereby delaying the implementation of the Law.

Protection will be granted to authors of literary, artistic and scientific works irrespective of the value, kind, purpose or expression of the work. Generally, the protection will be provided for works whose means of expression is writing, sound, drawing, image or film, and will include creative titles and computer software.

Qatar became a member of the Berne Convention for the Protection of Literary and Artistic Works on 5 July 2000;

(i) *Saudi Arabia*: The Copyright Law was issued by Royal Decree No. M/41 of 30 August 2003 and published in the Official Gazette No. 3959 of 19 September 2003. The implementing regulations of the Law were published in the Official Gazette of 4 June 2004 and entered into force on 2 August 2004.

The Law protects all types of intellectual works, whether literary, scientific or artistic. Foreign intellectual works are protected in accordance with the international conventions signed by Saudi Arabia. The Law incorporates stringent penalties to be imposed on infringers of intellectual property, including fines up to 250,000 Saudi Arabian riyals, closure of the violating establishment, confiscation of all copies of the infringing work, and imprisonment for a period not exceeding six months.

No copyright registration procedures are available in Saudi Arabia. According to the Berne Convention for the Protection of Literary and Artistic Works, registration in the home country extends to all member States.

However, any printed materials or computer programs can be distributed in Saudi Arabia only after receiving the approval of the Ministry of Information. For that purpose, a local distributor is essential, and the distributor must obtain the necessary approval locally.

Saudi Arabia became a member of the Berne Convention for the Protection of Literary and Artistic Works on 11 March 2004 and of the Universal Copyright Convention on 13 April 2004;

(j) *Syrian Arab Republic*: Copyright protection in the Syrian Arab Republic is governed by Law No. 12 of 2001. While the Syrian Copyright Protection Department (CPD) has started to process copyright applications, official fees have yet to be set.

The Syrian Arab Republic became a member of the Berne Convention for the Protection of Literary and Artistic Works on 11 June 2004;

(k) *United Arab Emirates*: Copyright in the United Arab Emirates is protected under the Copyright and Authorship Protection Law No. 7 of 2002. Generally, protection is provided for works whose means of expression is writing, sound, drawing, image and film, creative titles, or computer software and its applications and databases. Translation of original works is also protected.

The duration of the protection is for the lifetime of the author plus 50 years after death, or 50 years from the date of publication in cases of cinematographic works, works of corporate bodies and works published for the first time after the death of the author.

Unauthorized publication of a work of art is penalized by imprisonment and/or a fine of not less than 50,000 U.A.E. dirhams. A publisher who contravenes the instructions of the author through unauthorized addition, omission or modification can face imprisonment and/or a fine of not less than 10,000 U.A.E. dirhams.

The United Arab Emirates became a member of the Berne Convention for the Protection of Literary and Artistic Works on 14 July 2004;

(l) *Yemen*: While the unified Intellectual Property Rights Law No. 19 of 1994 stipulates protection for copyright in Yemen, the non-issuance of the implementing regulations has delayed the full implementation of the Law.

Box 3. Country code top-level domain names (ccTLD)

All ESCWA member countries have ccTLD registers that accredit the granting of the domain name. However, the ESCWA region still lacks provisions for domain name disputes. In Lebanon, for example, the Lebanese Domain Registry (LBDR) requests that any applicant for an “.lb” domain name must first apply to register the root domain (in the form “www.abcdefgh.com.lb”). The LBDR validates the relevant ccTLD as long as the corresponding trademark is valid. Hence, a dispute over the domain name can be litigated as a trademark infringement lawsuit before the court.

5. E-transactions, e-commerce and related fields

The major aspects of e-transactions are the validation and acceptance of the source that delivers an electronic document and of the content of such a document, as well as the authentication, validation and acceptance of e-signature.

The need to prove the authenticity of an electronic document is a major aim for legislators across the world, given that electronic documents represent the main tool for e-business in general, and for procedural legal requirements when two contracting parties, or sender and a receiver of electronic records, are dealing with each other over distance. The need to accept the validity of an electronic contract or document was aimed at facilitating commerce, especially in the light of the substantial growth in distance trading.

The legal aspects pertaining to e-transactions and e-commerce in countries outside the ESCWA region are summarized below.

In the United Kingdom, the Electronic Communications Act 2000 stipulates the provisions concerning the facilitation, among others, of electronic commerce and data storage. Under article 7 of that Law, the United Kingdom acknowledges as proof the legal power of an e-signature and the certification thereof, and the acceptance of such to admit the authenticity of the signed record or communication.

In the United States, one of the applicable laws in relation to e-signature is the Uniform Electronic Transactions Act (UETA), whose scope is inherently limited by the fact that it only applies to transactions related to business, commercial and consumer, and governmental matters. Consequently, transactions with no relation to the above-mentioned are not subject to this Act.

Moreover, the Electronic Signatures in Global and National Commerce Act (E-SIGN) regulates the activity of certificate authorities and sets the conditions for the practical application of digital signatures. However, E-SIGN does not correspond to the recommendations of the World Trade Organization (WTO), UNCITRAL and other influential organizations; and digital signature systems described therein are incompatible with international standards. For that reason, the Law will be amended to simplify the procedure of digital signatures.

In EU, article 5 of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures states that member countries “shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device: (a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and (b) are admissible as evidence in legal proceedings”. Moreover, member countries “shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is: in electronic form, or not based upon a qualified certificate, or not based upon a qualified certificate issued by an accredited certification-service-provider, or not created by a secure-signature-creation device”.¹⁴

¹⁴ Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures, *Official Journal of the European Communities* (19 January 2000). Available at: http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf.

The above article has set the base for European countries to amend or enact their related laws to follow similar principles. Examples include the Law of Electronic Signature in Switzerland, which defines the provisions for identifying the legal evidential power of e-signature, the rules to accept a signature, namely, certification and authentication thereof, and the rules to determine which authentication bodies or service providers have the authority to certify such authenticity; and the Signature Law of 2001 in Belgium, which stipulates the rules of the certification of service providers.

In countries of the ASEAN region, including Malaysia and Singapore, e-transaction laws have also been enacted and the topics treated therein are mainly the same as in international conventions and European countries. In Singapore, the Electronic Transactions Act of 1998 has elaborate articles concerning, among others, the recognition of foreign certification authorities, the revocation of certificates and the revocation without the consent of subscribers.

A glance at the e-commerce legislation in the ESCWA region reveals that those countries that have an applicable and applied law on e-commerce typically include the following legal topics: (a) electronic contracting at distance; (b) e-signature; (c) acceptance of e-documents (e-proof); and (d) e-banking and monetary transactions (e-transactions and e-payment). Other related e-commerce issues, including publicity over the Internet, are either mentioned in consumer protection laws or in other related legislations.

The countries of the ESCWA region that have applicable legislation in that area are set forth below:

(a) *Bahrain*: Law No. 28/2002 concerning electronic transactions stipulates provisions relating to e-signature, e-proof and accepting e-documents in transactions in general. Saving or keeping a document can be in an electronic form, and the Law recognizes the validity of the kept document in the electronic form. Moreover, the Law considers that e-documents have the same evidential power as written documents.

Article 6 recognizes the validity of e-signature as having an evidential power of expressing the will of the signatory on the signed document; articles 10 and 11 stipulate e-contract acceptance of expressing the consent and the execution of the content of the contract when such consent is sent and received in an electronic form; and article 12 defines the conditions of e-contracts in both business-to-consumer (B2C) and business-to-business (B2B) forms.

Summarizing the contents, the Law stipulates the acceptance of the following: (i) electronic forms when dealing between parties and the conditions for public entities to accept electronic forms and dealing; (ii) the evidential power of electronic records, being the same as for the written records; (iii) e-signature; (iv) electronic records as original ones, under the conditions stipulated in article 7 thereof; (v) saving and keeping the electronic documents and records; and (vi) e-contract;

(b) *Egypt*: Article 14 of the Law on E-Signature provides e-signatures with the same evidential legal power as written signatures in civil, commercial and administrative matters. Moreover, the acceptance of the e-signature and writing is confirmed; and hence, the legal evidential power is accepted to an e-signature and e-document in general when the signature relates to the signatory. The Law also specifies the terms for electronic certification processes and provides for penal sanctions of imprisonment and fines for offences of certification;

(c) *Iraq*: There is no evidence of legal provisions concerning e-transactions or e-commerce;

(d) *Jordan*: The E-Transactions Law No. 85 of 2001 applies to electronic transactions, electronic records, electronic signatures and any electronic data messages. In the area of electronic records, the Law stipulates the following:

- (i) Electronic transactions are approved by any government department or official institution, entirely or partially;
- (ii) The electronic record will fulfil its evidential weight, including its original form character, if it fulfils the following conditions: a. the information stated in the record can be retained

and stored in a manner whereby it may be referred to at any time; b. the possibility of retaining the electronic record in the form it had been generated, sent, received, or in any form that may prove that it accurately represents the information stated in the record during its generation, sending or receiving; and c. the information stated in the record is enough to verify its origin, receiving party, and date and time of transmittal and receipt.

Chapter 4 of the Law stipulates provisions relating to transferable electronic documents and defines those as being electronic documents to which the conditions of a negotiable bond shall apply; chapter 5 stipulates provisions relating to the electronic transfer of funds; and chapter 6 stipulates provisions relating to authentication and electronic signatures.

Article 31 of the Law recognizes the validity of an e-signature with the following provisos: (i) it is distinguishable and unique in its connection to the pertinent person; (ii) it is sufficient to identify its owner; (iii) it is generated in a manner or means specific to that person and under his control; and (iv) it is connected to the record related to him in a way that does not allow modification to that record after signing such without altering the signature. The Law is silent concerning other issues related to e-commerce;

(e) *Kuwait*: While there is no applicable legislation on e-commerce, a new draft law is pending enactment by Parliament. This draft, entitled the e-commerce law, stipulates the following main topics: (i) legal acknowledgment of e-documents; (ii) recognition of the validity and evidential power of e-signatures; (iii) acknowledgment of an e-document as an original; and (iv) acceptance of an e-document as a valid proof expressing consent in transactions and contracts. There is no specific date as to when that draft will be enacted;

(f) *Lebanon*: Lebanese legislation is silent on that issue. Electronic documents are not yet considered as proof per se; and procedural legislation must be amended before the electronic proof can stand as valid and have evidential weight. In the area of e-payment and money transfers, a set of decisions issued by the Central Bank regulates such transactions, in addition to those governing ATM systems. The said decision co-exists with applicable banking laws;

(g) *Oman*: There is no evidence of legal provisions concerning e-transactions or e-commerce;

(h) *Palestine*: Electronic documents, including letters and e-mails, have the same legal evidential power in commercial and civil matters according to article 19 of the Civil and Commercial Procedure Law No. 4 of 2001. That article also recognizes the legal evidential power of an e-mail. The same provisions have been reiterated in Arbitration Law No. 3 of the year 2000 and by Executive Decision No. 9 of 2004.

Moreover, article 26 of Law No. 12 of 2004 on financial securities provides the possibility of legally accepting electronic signatures as evidence;

(i) *Qatar*: There is no evidence of legal provisions concerning e-transactions or e-commerce;

(j) *Saudi Arabia*: A draft law on e-transactions is pending enactment by the legislative body in Saudi Arabia. That draft is aimed at: (i) accepting the validity of e-signatures and e-documents; (ii) enhancing the use of e-transactions at both local and foreign levels; and (iii) preventing the misuse and counterfeiting of e-signatures;

(k) *Syrian Arab Republic*: There is no evidence of legal provisions concerning e-transactions or e-commerce;

(l) *United Arab Emirates*: Federal and local laws in the United Arab Emirates and, more specifically, in Dubai, have in general accepted the electronic proof of documents and admitted the validity of e-contracts. Law No. 2 of 2002 (Dubai) stipulates the formation and validity of e-contracts. In the area of e-signatures, the Law stipulates that an e-signature stands as a written signature with the same evidential power when the said signature complies with authentication conditions mentioned in the Law;

(m) *Yemen*: Law No. 40 of 2006 concerning e-banking and e-payment stipulates, in chapter 4, the provisions of the legal effects of e-records, e-messages and e-signatures. According to those provisions, an electronic document of whatever nature, including letters, contracts and records, has the same legal validity as a written document in terms of proof, and is equally binding on the parties.

Concerning e-payment, the Law stipulates the provisions relating thereto in chapter 6, according to which electronic payment is accepted for the settlement of a debt and as a means of payment. Additionally, chapter 6 defines the rules that financial institutions have to abide by in money transactions; and chapter 7 provides for a legislator to set the rules of certification of an electronic record.

6. *Consumer protection*

Consumer protection is considered an area of public law that regulates private law relationships between individual consumers and commercial businesses that sell goods and services. Consumer protection covers product liability, privacy rights, unfair business practices, fraud, misrepresentation and a wide range of other consumer-business interactions.

Related laws deal with bankruptcy, credit repair, debt repair, product safety, service contracts, bill collector regulation, pricing, utility turnoffs and consolidation.

In EU, the European Council and Parliament issued Directive 97/7/CE of 20 May 1997 on the Protection of Consumers Regarding Distant Contracts, which stipulates the provisions that protect consumers from the misuse of credit cards, and defines the burden of proof borne by suppliers or businesses.

With the exception of Lebanon, most consumer protection laws are silent in the ESCWA region concerning the relationship between consumer and business when that relationship is made at distance. In Lebanon, the provisions of the law on consumer protection apply even when the relationship is carried out at distance. Consequently, while the legal protection for a consumer against fraudulent advertising, product safety or product recall can be sought under that law even when the relationship was carried out at distance, the burden of proof constitutes a hindrance along with the pertinent jurisdiction.

7. *Cyber crime*

This section offers a brief overview of the main international legal texts relating to cyber crime and the status of cyber crime laws in the ESCWA region.

The Convention on Cybercrime, issued by Council of Europe Treaty No. 185 (Budapest, 23 November 2001), defines the nature and main aspects of cyber and computer crime, as well as the need for cooperation and coordination between member countries in order to combat cyber crime and protect legitimate interests. The Convention acts as a deterrent by criminalizing actions that jeopardize the confidentiality, integrity and availability of computer systems, networks and computer data.

The cited offences are as follows:

- (a) Offences against the confidentiality, integrity and availability of computer data and systems, namely, illegal access, illegal interception, data interference, system interference and misuse of devices;
- (b) Computer-related offences, including computer-related forgery and computer-related fraud;
- (c) Content-related offences, including offences related to child pornography, xenophobia, racial content and harmful content;
- (d) Offences related to infringements of copyright and related rights.¹⁵

¹⁵ The Convention states that members must establish as criminal crimes infringements pursuant to national laws, the Berne Convention, Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement, the WCT (WIPO Copyright Treaty), the Rome Convention, and the WPT (WIPO Performances and Phonograms Treaty).

Moreover, the Convention addresses provisions relating to procedural law and to the investigation of the aforementioned offences.

Council of Europe Treaty No. 189 (Strasbourg, 28 January 2003), the Additional Protocol to the Convention on Cybercrime, Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer Systems, supplements the provisions of the Convention on Cybercrime and cites the following offences:

- (a) Dissemination of racist and xenophobic material through computer systems;
- (b) Racist and xenophobic motivated threat;
- (c) Racist and xenophobic motivated insult;
- (d) Denial, gross minimization, approval or justification of genocide or crimes against humanity.

The Convention and the Additional Protocol constitute the main international legal texts dealing with cyber crime and the European countries have amended or enacted their laws to be compliant with the Convention.

In the United Kingdom, the Computer Misuse Act of 1990 is the main applicable law for the prevention of cyber crime. The Act was created to criminalize unauthorized access to computer systems and to deter the use of computers for committing criminal offences or from impairing or hindering access to data stored in a computer. The basic offence is to attempt or achieve access to a computer or the data it stores by inducing a computer to perform any function with intent to secure access.

In the United States, cyber crime is subject to many laws and regulations in order to cover all possible unauthorized access to computer systems or attempts to fraud in connection with access devices. Relevant acts include the Access Device Fraud; the Computer Fraud and Abuse Act; the Can-Spam Act; and the Trade Secrets Act.

In the Arab region, such topics as sexuality, xenophobic and racial issues, discrimination, and religious and certain foreign political matters are considered to be under the purview of public order and any misbehaviour relating to any of the above is accountable under law and, more often than not, under criminal law. In the ESCWA region, while most countries have not yet enacted laws on preventing or combating computer crimes, some initiatives are beginning to show. The status of legislation in a selection of ESCWA countries is summarized below:

(a) *Bahrain*: Article 7 of Ministerial Decision No. 2 of 19 June 2006 concerning technical specifications accepted by official bodies for electronic transactions stipulates that electronic records cannot contain macros or scripts that can alter the record or the data contained therein;

(b) *Oman*: Articles 2 and 5 of Decree No. 72 on money laundering stipulates the means of controlling money transfers in order to uncover money laundering attempts;¹⁶

(c) *Palestine*: Executive Decision No. 269 of 2005 issued by the Council of Ministers concerning the confirmation of the general policies on the use of the computer and Internet in official institutions stipulates that access to pornography by official employees is misbehaviour. While that Decision does not stand as preventive against cyber crimes in general, it does regulate the use of computers against misuse in Government offices;

(d) *Saudi Arabia*: A new draft law, which is currently undergoing amendments before final enactment, is set to deal with such cyber crimes as hacking, assisting or covering terrorism, interception of transmissions, deletion, alteration, suppression, and change or destruction of computer data;

¹⁶ Most ESCWA member countries have laws to combat money laundering, which criminalize the illegal transfer of funds through electronic systems.

(e) *United Arab Emirates*: Federal Law No. 2 of 2006 stipulates combating cyber crime, with imprisonment and fines for the following offences:

- (i) Unauthorized or illegal access to a computer system or network which leads to the deletion, cancellation, destruction, dissemination, damage, redirection or suppression of computer data;
- (ii) Hindering or intercepting the access to a computer system or program;
- (iii) Counterfeiting any e-document recognized by the federal State;
- (iv) System interference: inserting what may cause a computer system or network to stop working adequately and to cause destruction, deletion, suppression or alteration of computer data or programs;
- (v) Deletion or alteration of medical results or diagnosis;
- (vi) Illegal intentional interception of transmissions of computer data;
- (vii) Using computer networks or any technical means to threaten a person or extort him to do or abstain from doing any act;
- (viii) Electronic theft using a computer system or network;
- (ix) Any offence against public morals using a computer system or network, including sexual, religious or private information relating to families, etc.;
- (x) Inciting prostitution;
- (xi) Human trafficking (advertising or assisting in);
- (xii) Illegal money transfers;
- (xiii) Assisting terrorism by creating web sites or decoys to cover operations.

According to the main principles of the Law, it is deemed unlawful to use the Internet or computer systems or networks for the following:

(a) To gain access intentionally and without authority or allow others to gain access to a web site or information system; access medical records, local and federal Government records and confidential Government information; intentionally stop or delay the Internet or computer system; and impede or intentionally prevent others from using the Internet or other computer systems, devices or technology;

(b) To erase, delete, remove, damage or amend software programs or data, or any information contained in such software programs or data;

(c) To commit fraud; induce, commit or facilitate slavery; sell or procure illegal drugs; launder money; tape communications; threaten or blackmail; organize or facilitate terrorist activities; and gain access to the particulars or serial numbers of credit cards or other electronic cards;

(d) To produce, prepare, distribute or save, with the intention of using or distributing, displaying or offering to third parties, anything that constitutes an offence to public morals, or to operate a business for such purposes;

(e) To persuade or instigate a male or female to perform an adulterous or grossly lewd act, or to assist in the performance of such an act, or the performing of such an act;

(f) To gain unauthorized access to a web site to alter, delete or inflict damage upon the web site, or to use the Uniform Resource Locator (URL) of the web site for unauthorized purposes;

(g) To deride Islam, Islamic religious beliefs, other religions or religious beliefs which are protected in accordance with Islamic doctrine, and abuse any of the recognized heavenly religions by using obscene language or embellishing signs.

Penalties and judicial procedures can be summarized as follows:

(a) A court will confiscate devices, software or tools used to commission a crime and any money generated by crime specified under the Law;

(b) A court will deport foreign nationals who commit an offense under the Law;

(c) A court may apply a more severe penalty if an offence has been committed under another law or code that provides for a more severe penalty.

The Federal Law complies with almost every cyber crime law as cited in the European Convention on Cybercrime, with the exception of articles relating to copyright and IPRs in general, which the United Arab Emirates have protected in separate IPR laws. Those IPR laws are still in force and prevail over the provisions of Federal Law No. 2 of 2006 when there has been an infringement of an IPR, whether online or through a computer system. Despite the fact that such a crime is considered a cyber crime, the lack of appropriate provisions in the Federal Law is compensated by existing IPR laws.

Furthermore, cyber crimes are generally prosecuted under criminal law provisions when the national legislation of a given country lacks the adequate cyber crime legislation. The main issue in such an event is the application of criminal procedural law in finding evidence of the crime itself, as the evidence would also be electronic in most of the cases. Thus, such cybercrimes are crimes committed on the computer system or network, not usual crimes committed using a computer system or network. For example, fraud can be committed using e-mails in order to deceive victims. Such a crime is not labelled a cyber crime merely because the tool of the fraud included a computer system or network, or the use of electronic means to facilitate the commitment of the crime itself.

II. RECOMMENDATIONS FOR DRAFTING A MODEL CYBER LAW IN THE ESCWA REGION

Those countries of the ESCWA region that still lack cyber legislation or have not yet amended their current laws to include cyber-related legal aspects and issues, need to reach a state where issues pertaining to cyber legislation are adequately regulated, thereby progressing in the electronic evolution and the use of computer systems and networks. The recommendations set below are intended to clarify, to the most possible extent, the plan that those countries could follow to achieve the stated goals.

The enactment of a cyber-related law or a set of legislative decrees at a national level is not the only alternative to regulate cyber-related legal issues. In fact, other alternatives are available, namely, to substitute the enactment of a national law or to assist in the enactment thereof by reducing the amount of prerequisites that are necessary for the enactment process.

With the exception of some ESCWA member countries, the region in general still lacks proper legislation that deals directly with cyber-related topics. That can be attributed to various reasons, including: (a) the underestimation of the importance of and need for such legislation by the legislative bodies of a country; (b) the fact that the judicial body does not have a backlog of cyber-related cases; (c) that the judicial body has been able to use the existing laws and provisions by analogy and broad interpretation to overcome or to adjudicate cases and lawsuits involving or having a cyber character.

In those ESCWA member countries where the process of enacting cyber legislation has begun, there is evidence to suggest that such enactments are related in large part to an increase in foreign investment inside the country over the past decade, and that such investment has increasingly used electronic means. That influence has prompted national legislators to actively review existing laws and to amend the provisions thereof by enacting new cyber legislation in such specific fields as e-transactions, e-proof and e-signature.

Notwithstanding the above, waiting for an increase in foreign investment in order to enact cyber legislation does not represent the best approach for those countries still lacking such legislation. Rather, the opposite argument could be more persuasive, with foreign investment being attracted to a country that has already enacted cyber legislation.

Consequently, the availability of adequate cyber legislation is one factor that could contribute to the economic growth of a country and simplify litigation before the courts.¹⁷

As the current situation stands, the countries of the ESCWA region can be grouped into three categories, namely: (a) countries with substantial initiatives on cyber legislation, including Bahrain and the United Arab Emirates; (b) countries and territory with some cyber legislation, including Egypt, Jordan, Palestine and Yemen; and (c) countries with no cyber legislation, including Iraq, Kuwait, Lebanon, Oman, Qatar, Saudi Arabia and the Syrian Arab Republic.¹⁸

While the countries in the first two categories have dealt with various cyber legislation issues, some major topics still lack legislative embodiment even in those countries. Those topics are summarized below.

(a) *Data protection*: While the United Arab Emirates issued the Data Protection Law of 2007, it is not a federal law and applies only in the jurisdiction of the Dubai International Financial Centre (DIFC).

¹⁷ Within that context, litigation is facilitated given that judges are not required to analyse existing cyber laws. By contrast, where cyber legislation has not been enacted, topics of a cyber-legal nature must necessarily be interpreted using less compatible laws.

¹⁸ The lack of cyber legislation is understood as the absence of a cyber law. However, some of those countries have either drafted laws that are pending enactment, or have regulations or decisions issued by central banks or ministries concerning such cyber-related legal topics as e-payment.

Other countries still lack adequate legislation protecting data storage and processing. Some articles have been introduced, including telecommunications laws, under which secrecy of communication is not to be breached. However, those provisions, where they exist, do not reach the required level of protection of data;

(b) *Cyber crime*: Cybercrime, defined as both computer-related crime and content-related crime, is still a topic that is comparatively neglected in the ESCWA region. The only initiative was made by the United Arab Emirates in the enactment of Federal Law No. 2 of 2006 on Combating Information Technology Crimes, in compliance with EU cybercrime laws, which punishes both content-related and computer-related crimes;

(c) *Censorship and freedom of expression*: For national political reasons, that issue is totally and intentionally ignored in the countries of the ESCWA region;

(d) *Privacy on the Internet*: There is no evidence of any legislation in any ESCWA member country concerning the protection of privacy on the Internet. In the absence of adequate legislation, the courts usually deal with privacy-related offences through intellectual property laws or penal laws;

(e) *E-commerce*: The countries of the ESCWA region lack legislation on consumer-to-consumer (C2C) and business-to-consumer (B2C) relationships. E-commerce is closely related to trade in general, and thus is also subject to the provisions of commercial laws. However, such laws need to be amended in order to implement legal issues that are solely related to e-business.¹⁹ While some of the major issues could be treated within e-transaction laws, including e-signature and attribution, such topics as consumer protection and advertising on the Internet have not been addressed. Advertising on the Internet has not yet been legislatively treated in the countries of the ESCWA region;

(f) *Telecommunications*: While the countries of the ESCWA region have enacted laws regulating telecommunications, there is no legislation concerning electronic telecommunications. By contrast, the countries of EU have embodied articles in their telecommunications laws that provide for rules concerning electronic communications. In France, for example, the Code governing postal communications establishes provisions concerning communications in electronic forms.

In order to be closer to foreign legal integration of cyber legislation, the countries of the ESCWA region need to address the above topics; either by ratifying relevant international conventions; or by enacting national laws that are compliant with international directives, agreements and/or national laws. Specifically, those ESCWA member countries without cyber legislation could follow the process described below.

Generally, most national constitutions recognize international conventions and treaties, once the country is a signatory, as part of the local legislation and may take precedence over locally enacted laws. Therefore, countries without cyber laws could start by ratifying an international treaty or convention that treats a cyber-related topic, including, for example, e-signature or e-proof. In so doing, a country would only have to amend existing laws in order to comply with the provisions of the treaty or convention and to delete any contradictions therewith.

The first step would be to assess the legislation status of the country in question in order to set a clear list of the laws that need to be amended in order to comply with cyber-related legal topics, and to define what cyber-related topics have to be subject to a nationally enacted law, in the event that no available international or regional treaty or convention can be ratified to complete the local legislation on that specified issue.

As mentioned above, the need for a cyber-related legislation, whether through ratification of an international treaty or convention or enactment of a national law, will usually be backed by the judicial system and the interest groups, who, if adequately informed, could lobby legislators to proceed with the enactment process. Consequently, the main focus for attracting the attention of such groups is to create,

¹⁹ The provisions of existing laws on consumer protection could apply to C2C or B2C relationships.

among others, working plans through workshops, seminars for lawyers and judges, and conferences for interest groups. Those working plans could help to boost the knowledge of both the interest groups and the legislators of the necessity of such a law.

Subsequently, legislators may opt for one out of three approaches in order to present a cyber law, namely: (a) to draft a local law; (b) to ratify an international treaty, thereby saving time in terms of drafting a local law; and (c) to adopt a model law that is available on a regional or international level.²⁰

A. MECHANISM FOR ENACTING CYBER LEGISLATION

The working plan for enacting a new law is set forth below:

(a) *Creating a specialized focus group*: Such a group is usually formed by the following: (i) concerned ministry professionals in a given field, including the ministries of trade, economy and telecommunications; (ii) professionals from ICT companies and organizations; and (iii) legal professionals, including lawyers and legal counsellors in related fields, with knowledge and experience of the subject field. That group could establish a template comprising a checklist of the main topics that deal with the subject of the law, for example e-commerce, data protection or cyber crime. That checklist can be expanded and/or amended in the light of foreign laws on the same subject or of international treaties or conventions.

The focus group shall consult international conventions dealing with the subject of the law to be enacted, and foreign initiatives and laws on the same subject. Such a review of foreign laws must also comprise the original law as enacted by the foreign State and any subsequent amendments, so as to allow lessons to be drawn from necessary revisions and amendments after the law was enacted. Moreover, the focus group is encouraged to review the reasons and necessities for enacting the law in order to ascertain whether similar needs apply locally.

Finally, the focus group will be able to put down recommendations concerning the main topics that are to be treated in the law;

(b) *The model law and focus group*: When the recommendations of the first focus group are set, a preliminary draft of the law, referred to as a model law, is completed. The focus group is then enlarged and additional professionals are invited to discuss the model law, article by article. Those discussion boards usually include professionals from both the public and private sectors who represent the main subjects to the application of the provisions of the law upon enactment, namely, Internet service providers, intellectual property law firms, telecommunications firms, judiciary police officers combating cyber crime, and officials of chambers of commerce dealing with issues related to e-commerce.

After the completion of the study and discussion meetings, the focus group would have a draft law ready to be submitted to the ministry concerned;

(c) *Interviews and workshops*: When the draft law is ready, interviews with key persons will be needed in order to discuss the law and its projected impact on the public and private sectors. Additionally, workshops with members of parliament should be held in order to acquaint them with the draft. Such interviews and workshops are aimed at explaining the law and building the understanding thereof to the members of the parliamentary committee that will study the draft and make necessary amendments, thereby making it compliant with existing legislation and ensuring that the provisions and procedures of the new draft do not contradict established laws;

²⁰ Within that context, the League of Arab States drafted and adopted a model law, entitled "Internet Law", in which it treated the following main sections: e-storage (digital storage), computer databases, e-transactions, e-commerce and cyber crime or, more specifically, crime through the Internet. That model law could be a basis for study and discussion among members of the focus group.

(d) *Discussion sessions*: The final phase before enacting the law relates to discussion sessions concerning the draft. Those sessions will group experts in the related fields and aim at ensuring the draft law covers all possible situations that can occur from the application of its provisions;

(e) *Regional directives*: The example of the EU Council regarding the issuance of directives relating to cyber legislation issues represents a paradigm for enhancing the state of cyber legislation in the ESCWA region. The League of Arab States or the Gulf Cooperation Council (GCC) could represent adequate bodies to issue directives concerning such topics as cyber crime or data protection. Naturally, while these directives could not be applied as international treaties that are enforceable as local laws, member countries could be given set time periods in order to amend their existing laws or introduce regulations that are compliant with the provisions of such directives. Essentially, enacting local laws based on directives could be an easier course, given that such directives would already have been issued based on focus groups and studies.

B. CONCLUSIONS

This study provided an overview of the cyber laws enacted and in force in the ESCWA region; and of the initiatives currently underway, aimed at achieving and completing cyber legislation and at adapting existing laws to international texts and directives.

Some countries of the region have already proceeded with the enactment and promulgation of various cyber laws, particularly countries of the GCC and Egypt. Others are still either awaiting the legislative body to pass cyber legislation, or studying and drafting the text of such laws.

This study revealed that, in general, the countries of the ESCWA region are following international and foreign laws as models when drafting national legislation. That is highlighted by the laws enacted in the most advanced countries of the ESCWA region regarding cyber issues, principally the Computer Crime Law and the Data Protection Law of the United Arab Emirates (Dubai).

In the future, the countries of the region could reach a point where cyber-related legal topics are addressed either by the ratification of international conventions, or through the enactment of national laws. The initiatives carried out by the European Community, as well as the acquired experience of other international organizations, could help to encourage ESCWA member countries in terms of the enactment of national cyber laws. Furthermore, those ESCWA member countries seeking to join WTO will have to comply with the standards required by the Organization and will have to amend their laws in order to meet those standards, including, for example, by enacting intellectual property laws that are compliant with the TRIPS Agreement.

Annex I

LIST OF INTERNATIONAL AND REGIONAL CONVENTIONS

	Title of convention	Web link
Cyber crimes		
	Convention on Cybercrime (Budapest, 23 November 2001)	http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm
	Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (Strasbourg, 28 January 2003)	http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=189&CM=8&DF=7/6/2007&CL=ENG
Protecting personal data		
	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Strasbourg, 28 January 1981)	http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm
	Amendments to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Strasbourg, 15 June 1999)	http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm
	Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding Supervisory Authorities and Transborder Data Flows (Strasbourg, 8 November 2001)	http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm
	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML
Electronic communications		
	Draft declaration on the freedom of communication on the Internet (Strasbourg, 8 April 2002)	http://www.humanrights.coe.int/media/documents/Draftdeclaration.rtf
	Declaration on Freedom of Communication on the Internet (adopted by the Committee of Ministers on 28 May 2003 at the 840 th Meeting of the Ministers' Deputies)	http://wcd.coe.int/ViewDoc.jsp?id=37031
	Community-COST Concertation Agreement on a Concerted Action Project in the Field of Teleinformatics (COST Project 11 bis)	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:21981A0122(01)
	Guidelines for the Regulation of Computerized Personal Data Files, adopted by General Assembly resolution 45/95 of 14 December 1990	http://www.unhchr.ch/html/menu3/b/71.htm
	Bucharest Declaration on Combating Counterfeiting and Piracy (12 July 2006)	http://www.interpol.int/Public/FinancialCrime/IntellectualProperty
	Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications)	http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf
	Cooperation Agreement between the European Economic Community and the Kingdom of Sweden on the Interconnection of the Community Network for Data Transmission (Euronet) and the Swedish Data Network for Information-Retrieval Purposes (14 December 1981)	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?

	Title of convention	Web link
Computer programs		
	OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (2002)	http://www.oecd.org/document/48/0,3343,en_2649_34255_15582250_1_1_1_1,00.html
	Directive 91/250/EEC of 14 May 1991 on the Legal Protection of Computer Programs	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31991L0250:EN:NOT
	Council Resolution 96/C 376/01 of 21 November 1996 on New Policy Priorities regarding the Information Society	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996Y1212(01):EN:NOT
	Council Framework Decision 2005/222/JHA on Attacks against Information Systems	http://cryptome.org/eu-antihack.htm
	IT Security and Crime Prevention Methods	http://www.interpol.int/Public/Technologycrime/Crimeprev/Itsecurity.asp
E-commerce		
	Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures	http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf
	Recommendation on the Legal Value of Computer Records (1985), the United Nations Commission on International Trade Law (UNCITRAL)	http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1985Recommendation.html
	United Nations Convention on the Use of Electronic Communications in International Contracts, adopted by the General Assembly on 23 November 2005	http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html
	Rules for Electronic Bills of Lading (Comite Maritime International)	http://www.comitemaritime.org/cmidsocs/rulesebla.html
	Agreement between the European Economic Community and the Republic of Austria on Trade Electronic Data Interchange Systems (21 December 1989)	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31989D0689:EN:HTML
Intellectual property		
	Community-COST Concertation Agreement on a Concerted Action Project in the field of Artificial Intelligence and Pattern Recognition (COST Project 13)	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:21985A1203(01
	Convention for the Protection of Producers of Phonograms against an Unauthorized Duplication of their Phonograms, adopted by WIPO 1971	http://www.wipo.int/treaties/en/ip/phonograms/trtdocs_wo023.html
	WIPO Copyright Treaty (WCT), adopted in Geneva on 20 December 1996	http://www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html
	WIPO Performances and Phonograms Treaty (WPPT), adopted in Geneva on 20 December 1996	http://www.wipo.int/treaties/en/ip/wppt/trtdocs_wo034.html
	International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention 1961)	http://www.wipo.int/treaties/en/ip/rome/trtdocs_wo024.html
	Berne Convention for the Protection of Literary and Artistic Works, as amended on 28 September 1979	http://www.wipo.int/treaties/en/ip/berne/trtdocs_wo001.html

Annex III

LIST OF CYBER TOPICS

A. PROTECTION OF INDIVIDUAL AND PERSONAL DATA

1. *Data protection principles*
 - Data shall be fair and lawful
 - Data shall be specific and for lawful purposes
 - Data shall be adequate
 - Data shall be accurate
 - Protection of security of data
 - Protection of the rights and freedom of data
2. *Data processing by public bodies*
 - Collection of data
 - Storage, modification and use of data
 - Communication of data to public bodies
 - Communication of data to private bodies
3. *Rights of the data subject*
4. *Protection of automatic processing of data*
 - Data subject/quality of data/categories of data
 - Data integrity
 - Accuracy and completeness of data
 - Personal data
 - Right of access to personal data
 - Automatic processing
 - Right to prevent processing likely to cause damage or distress
 - Right to prevent processing for purposes of direct marketing
 - Automated data file
 - Rights in relation to automated decision taking
 - Controller of the file
 - Prohibition on processing without registration
 - Notification by data controllers
 - Registration of notifications
 - Duty to notify changes
5. *Trans-border data flows*

B. PROTECTION OF PRIVACY AND FREEDOM OF INFORMATION IN THE ELECTRONIC COMMUNICATIONS SECTOR

- Confidentiality of communications
- Data retention
- Unsolicited electronic messages (“spamming”)

- “Cookies”
- Public directories

C. COPYRIGHTS, NEIGHBOURING RIGHTS AND INDUSTRIAL PROPERTY RIGHTS WITHIN THE INFORMATION SOCIETY

- Computer programs
- Compilation of data (database)
- Right of distribution
- Right of rental
- Right of communication to the public
- Right of management information
- Reproduction rights
 - for authors, of the original and copies of their works
 - for performers, of fixations of their performances
 - for phonogram producers, of their phonograms
 - for producers of the first fixation of films, in respect of the original and copies of their films,
 - for broadcasting organizations, of fixations of their broadcasts, whether those broadcasts are transmitted by wire or over the air, including by cable or satellite
- Right of communication
 - performers, of fixations of their performances
 - for phonogram producers, of their phonograms
 - for the producers of the first fixation of films, in respect of the original and copies of their films
 - for broadcasting organizations, of fixations of their broadcasts, regardless of the method of transmission
- Distribution rights

D. ELECTRONIC TRANSACTION

- Electronic record
- Electronic signature
- Attribution
- Legal recognition of electronic records

E. ELECTRONIC COMMERCE

- Electronic contracting (business-to-business, business-to-consumer)
 - Remote contracts
 - Consumer protection
- Publicity on Internet
 - Publicity technique
 - Publicity methods (World Wide Web, e-mail, chatrooms, forums of discussion)
 - Legal status of publicity on Internet
 - Identification principle

- Transparency of truthfulness of information
- Misleading advertisement

- Electronic proof
- Electronic signature
- Electronic payment

- Electronic transfer
- Exchange letters, payment cards
- Establishments of plastic money
- Combat money laundering

F. CYBER CRIMES

1. *Internet crimes*

- Crimes related to persons (pornography, minors)
- Crimes related to consumer goods
- Crimes related to public sector
- Crimes related to information and electronic communications

2. *Computer crimes*

- Computer system
- Computer program
- Computer data
- Computer devices

Annex IV

COMPARATIVE MATRIX OF CYBER LEGISLATION

A. THE ESCWA REGION

Bahrain	United Arab Emirates (Dubai)	Egypt	Iraq	Jordan	Kuwait	Lebanon	Oman	Palestine	Qatar	Saudi Arabia	Syrian Arab Republic	Yemen
I. Protection of individual and personal data												
Telecommunications Law No. 48/2002 Articles 39, 40 and 41	Data Protection Law 2007	Telecommunications Law No. 10/2003			Draft law on e-commerce	Draft law on e-commerce Section 2		Telecommunications Law No. 3/1996	Decree Law No. 34/2006 on the promulgation of the Telecommunications Law	Telecommunications Law of 2001		
I. Protection of individual and personal data: data processing by public bodies												
				Temporary Law on Applying IT Resources in Governmental Entities 2003								
II. Protection of privacy and freedom of information in the electronic communications sector												
Decision No. 2/2006 Electronic Transactions	Data Protection Law 2007					Draft law on e-commerce Section 2						
	Law No.2/2002 E-commerce and E-transactions											
III. Copyrights, neighbouring rights and industrial property rights												
Law No. 22/2006 Copyright and Neighbouring Rights	Law 2002 Copyright and Neighbouring Rights Articles 1, 7 and 38	Law No. 82/2002 Protection of Intellectual Property Rights	Order No.83/2004 amending Copyright Law	Copyright Law No. 22/1992	Copyright Law No. 5/1999	Copyright Law No. 75/1999	Copyright Law Royal Decree No. 37/2000		Copyright Law No. 25/1995	Copyright Law-Royal Decree No. M/41/2003	Copyright Law No. 12/2001	Unified Intellectual Property Rights Law No. 19/1994
	Amendment to Trademarks Law 2002					Draft Law on e-commerce Section 8						
	Law No. 1/2000 Dubai Free Zone of Technology, E-commerce and Information											
IV. Electronic transactions												
Decree No. 28/2002 Electronic Transactions	Law No. 2/2002 E-commerce and E-transaction			Law No. 85/2001 E-transactions						Draft law on e-transactions		

Bahrain	United Arab Emirates (Dubai)	Egypt	Iraq	Jordan	Kuwait	Lebanon	Oman	Palestine	Qatar	Saudi Arabia	Syrian Arab Republic	Yemen
V. Electronic commerce: 1. Electronic contracting												
V. Electronic Commerce: 1. Electronic contracting - Contract at distance												
Decree No. 28/2002 Electronic Transactions	Law No.2/2002 E-commerce and E-transactions				Draft law on e-commerce	Draft law on e-commerce, Section 7			Draft law on e-commerce	Draft law on e-transactions	Draft law on e-signature	Law No. 40/2006 E-payment and E-banking
Law No. 13/2006 E-commerce	Law No. 1/2000 Dubai Free Zone of Technology, E-commerce and Information											
V. Electronic commerce: 1. Electronic contracting - Consumer protection												
Decree No. 28/2002 Electronic Transactions						Draft law on e-commerce, Section 7			Draft law on e-commerce			
Law No. 13/2006 E-commerce						Decree No. 13068/2004 Consumer Protection						
Decree No. 28/02 Electronic Transactions												
V. Electronic commerce: 2. Electronic proof												
Decree No. 28/2002 Electronic Transactions Articles 5, 7, 8 and 9	Law No. 2/2002 E-commerce and E-transactions	Law 2004 E-signature		Law No. 85/2001 E-transactions	Draft law on e-commerce	Draft law on e-signature Section 4		Law No. 4/2001 Civil and Commercial Evidence Article 19	Draft law on e-commerce	Draft law on e-transactions	Draft law on e-signature	Law No. 40/2006 E-payment and E-banking
Decision No. 2/2006 Electronic Transactions	Customs Law of 1998	Law No. 25/1968 Civil and Commercial Evidence						Decision No. 39/2004 concerning Arbitration Law Article 19				
Law No. 13/2006 E-commerce	Law 2006 Civil and Commercial Evidence Articles 1 and 17											
	Land Registry Law (Dubai) 2006 Articles 2, 7 and 8											
V. Electronic commerce: 3. Electronic signature												
Decree No. 28/2002 Electronic Transactions Article 6	Law No. 2/2002 E-commerce and E-transactions	Law 2004 E-signature		Law No. 85/2001 E-transactions	Draft law on e-commerce	Draft law on e-commerce Section 3		Law No. 12/2004 Financial Securities Article 26	Draft law on e-commerce	Draft law on e-transactions	Draft law on e-signature	Law No. 40/2006 E-payment and E-banking
Law No. 13/2006 E-commerce												
Decision No. 2/2006 Electronic Transactions												

Bahrain	United Arab Emirates (Dubai)	Egypt	Iraq	Jordan	Kuwait	Lebanon	Oman	Palestine	Qatar	Saudi Arabia	Syrian Arab Republic	Yemen
V. Electronic commerce: 4. Electronic payment/electronic transaction												
Decree No. 28/2002 Electronic Transactions	Law No. 2/2002 E-commerce and E-transactions			Law No. 85/2001 E-transactions		Draft law on e-commerce Section 5			Draft law on e-commerce	Draft law on e-transactions		Law No. 40/2006 E-payment and E-banking
Law No. 1320/2006 E-commerce						Monetary and Credit Law 1963 Articles 33, 70, 80 and 174 Law No. 133/1999						
						Circular No. 9217/2005 Electronic Banking						
						Circular No. 8430/2003 Electronic Banking and Financial Transactions						
						Circular No. 8216/2002 ATMs and Credit Cards						
						Circular No. 8341/2003 Electronic Clearing House for Credit Cards and Payments Cards						
						Circular No. 8283/2002 List of Credit Cards Used in Lebanon						
						Circular No. 7299/1999 ATM & Payment Cards						
V. Electronic commerce: 5. Publicity on Internet												
V. Electronic commerce: 6. Domain names/Internet												
Decree No. 28/2002 Electronic Transactions								Draft law concerning the Palestinian national body for ccTLD		Decision dated 17/6/06 Universal Access and Universal Service Policy		
Law No. 13/2006 Amending Decree No. 28/2002								Decision No. 35/2004 Accessing the Internet through Government Computer Centre		Decision No. 6667 Conditions for Practicing IT and Telecommunications Counselling		
Law No. 13/2006 E-commerce								Decision No. 74/2005 National Strategy for Telecommunications and Information Technology				

Bahrain	United Arab Emirates (Dubai)	Egypt	Iraq	Jordan	Kuwait	Lebanon	Oman	Palestine	Qatar	Saudi Arabia	Syrian Arab Republic	Yemen
Decision No. 2/2006 Electronic Transactions								Decision No. 269/2005 Use of Computer and Internet in Official Institutions				
VI. Cyber crimes: 1. Internet crimes												
	Federal Law No. 2/2006 Combating Information Technology Crimes	Law 2004 E-signature		Law No. 85/2001 E-transactions		Draft law on e-commerce Section 6			Draft law on e-commerce	Draft law on combating informatics crimes	Draft law on e-signature	Law No. 4020/2006 E-payment and E-banking
	Law No. 2/2002 E-commerce and E-transactions					Law No. 318/2001 Combating Money Laundering				Draft law on e-transactions		
	Law No. 1/2000 Dubai Free Zone of Technology, E-commerce and Information					Circular No. 7818/2001 Supervision of Banking and Financial Operations in order to Combat Money Laundering						
	Anti-Terrorism Law 2004											
VI. Cyber crimes: 2. Computer crimes												
	Federal Law No. 2/2006 Combating Information Technology Crimes					Decision No. 4 of 25/5/2006 Concerning Computer Programs and Combating Piracy						

B. INTERNATIONAL

EU countries						European Council	North America		ASEAN		UN/UNICTRAL	Conventions	
Belgium	France	Germany	Luxemburg	Sweden	Switzerland	United Kingdom	EC	Canada	United States of America	Malaysia			Singapore
I. Protection of individual and personal data													
Loi réglant services financiers à distance et de la directive vie privée & communications électroniques	Loi n° 2004-801 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel	Federal Data Protection Act of 20 December 1990		Personal Data Act 1998:204		Data Protection Act 1998	Directive 2002/58/EC Data Protection in the Electronic Communications Sector	Personal Information Protection and Electronic Documents Act	The Privacy Act of 1974			Guidelines concerning Computerized Personal Data Files	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Strasbourg, 28 January 1981)
	Loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés						Regulation No. 45/2001 on the Protection of Individuals with regard to the Processing of Personal Data						Amendments to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, (Strasbourg, 15 June 1999)
	Loi n° 2004-575 pour la confiance dans l'économie numérique						Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data						Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Strasbourg, 8 November 2001)
I. Protection of individual and personal data: data processing by public bodies													
		Federal Data Protection Act of 20 December 1990					Recommendation No. 87 concerning the Regulating of the Use of Personal Data in the Police Sector						
II. Protection of privacy and freedom of information in the electronic communication sector													
Loi réglant services financiers à distance et de la directive vie privée et communications électroniques	Loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés	Federal Data Protection Act of 20 December 1990		Personal Data Act 1998:204		Data Protection Act 1998	Regulation No. 45/2001 on the Protection of Individuals with regard to the Processing of Personal Data	Personal Information Protection and Electronic Documents Act	The Privacy Act of 1974				Draft declaration on freedom of communication on the Internet, (Strasbourg, 8 April 2002)
	Loi n° 2004-575 pour la confiance dans l'économie numérique						Directive 2002/58/EC Data Protection in the Electronic Communications Sector		United States Code, Title 5 Section 552 Electronic Freedom of Information Act Amendments of 1996				Community-COST Concertation Agreement on a Concerted Action Project in the Field of Teleinformatics
	Loi n° 2004-801 relative à la protection des personnes physiques						Council Decision 92/242/EEC in the field of Information Security						

EU countries							European Council	North America		ASEAN		UN/UNICTRAL	Conventions
Belgium	France	Germany	Luxemburg	Sweden	Switzerland	United Kingdom	EC	Canada	United States of America	Malaysia	Singapore		
	à l'égard des traitements de données à caractère personnel												
							Directive 97/66/EC concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector						
							Regulation No. 460/2004 establishing the European Network and Information Security Agency						
III. Copyrights, neighbouring rights and industrial property rights													
Loi transposant en droit belge la Directive européenne 2001/29/CE -droit d'auteur et des droits voisins dans la société de l'information	Loi n° 2006-961 relative au droit d'auteur et aux droits voisins dans la société de l'information					-	Directive 2001/29/EC on the Harmonization of Certain Aspects of Copyright and Related Rights in the Information Society		Federal Criminal Statutes Protecting Intellectual Property Rights 17 U.S.C. 506, 1201 to 1205, 506 18 U.S.C. 2318, 2319, 2319A, 2320, 1831 to 1839, 497				European Convention for Patent Application (Paris, 11 December 1953)
							Recommendation No (88) 2 on Piracy in the field of Copyright and Neighbouring Rights						European Convention relating to questions on Law on Copyright and Neighbouring Rights
							EC Green Paper 1995 on Copyright and Related Rights in the Information Society						WIPO Copyright Treaty (WCT)
													WIPO Performances and Phonograms Treaty (WPPT)
													Rome Convention for the Protection of Performers (1961)
													Berne Convention for the Protection of Literary and Artistic Works
													Geneva Convention for the Protection of Producers of Phonograms

EU countries							European Council	North America		ASEAN		UN/UNICTRAL	Conventions
Belgium	France	Germany	Luxemburg	Sweden	Switzerland	United Kingdom	EC	Canada	United States of America	Malaysia	Singapore		
IV. Electronic transactions													
Loi relative au moyen d'instruments de transfert électronique de fonds						Electronic Communications Act 2000		Electronic Information and Documents Act	Uniform Transactions Act 1999		Electronic Transactions Act 1998		
								Personal Information Protection and Electronic Documents Act	U.S. Code, Title 18 Chapter 121 Stored Wire and Electronic Communications and Transactional Records Access				
									Digital Millennium Copyright Act				
V. Electronic commerce: 1. Electronic contracting													
V. Electronic commerce: 1. Electronic contracting - Contract at distance													
La nouvelle loi belge sur le commerce électronique			Règlement relatif aux signatures électroniques, au paiement électronique et à la création du comité 'commerce électronique'				Directive 97/7/CE concernant la protection des consommateurs en matière de contrats à distance		Uniform Transactions Act 1999			United Nations Convention on the Use of Electronic Communications in International Contracts	
Loi fixant les signatures électroniques et les services de certification							The Electronic Commerce (EC Directive) Regulations 2002		Electronic Signatures in Global and National Commerce Act			Loi type de la CNUDCI sur le commerce électronique	
V. Electronic commerce: 1. Electronic contracting - Consumer protection													
							Directive 97/7/CE concernant la protection des consommateurs en matière de contrats à distance		Electronic Signatures in Global and National Commerce Act				
	Décret n° 2005-1450 relatif à la commercialisation à distance de services financiers auprès des								Anti-cybersquatting Consumer Protection Act				

EU countries						European Council	North America	ASEAN		UN/UNICTRAL	Conventions	
Belgium	France	Germany	Luxemburg	Sweden	Switzerland	United Kingdom	EC	Canada	United States of America			Malaysia
V. Electronic commerce: 2. Electronic proof												
La nouvelle loi belge sur le commerce électronique			Règlement relatif aux signatures électroniques, au paiement électronique et à la création du comité "commerce électronique"		Loi Federale sur les services de certification dans le domaine de la signature électronique	Electronic Communications Act 2000			Uniform Transactions Act 1999	Digital Signature Regulations 1998	Electronic Transactions Act 1998	
Loi fixant les signatures électroniques et les services de certification	Arrêté relatif à la qualification des prestataires de services de certification électronique								Electronic Signatures in Global and National Commerce Act			
Arret royal organisant le contrôle et l'accréditation des prestataires de service de certification qui délivrent des certificats qualifiés												
V. Electronic commerce: 3. Electronic signature												
La nouvelle loi belge sur le commerce électronique			Règlement relatif aux signatures électroniques, au paiement électronique		Loi Federale sur les services de certification dans le domaine de la signature électronique	Electronic Communications Act 2000	EC: Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in particular Electronic Commerce, in the Internal Market		Uniform Transactions Act 1999	Digital Signature Regulations 1998	Electronic Transactions Act 1998	56/80 Model Law on Electronic Signatures
Loi fixant les signatures électroniques et les services de certification							Directive 1999/93/EC on a Community Framework for Electronic Signatures		Electronic Signatures in Global and National Commerce Act			51/162 Model Law on Electronic Commerce
V. Electronic commerce: 4. Electronic payment/electronic transaction												
Loi réglant services financiers à distance et de la directive vie privée et communications électroniques.	Décret n° 2005-1450 relatif à la commercialisation à distance de services financiers auprès des consommateurs		Règlement relatif aux signatures électroniques, au paiement électronique				Commission Recommendation 87/598/EEC, concerning a European Code of Conduct relating to Electronic Payments		Electronic Signatures in Global and National Commerce Act			
Loi modifiant le Code de la taxe sur la valeur ajoutée Facture électronique	Règlement No. 2002/13 relatif à la monnaie électronique et aux						Commission Recommendation 97/489/EC concerning Transactions by					

EU countries							European Council	North America		ASEAN		UN/UNICTRAL	Conventions
Belgium	France	Germany	Luxemburg	Sweden	Switzerland	United Kingdom	EC	Canada	United States of America	Malaysia	Singapore		
- 2004	établissements de monnaie électronique						Electronic Payment Instruments						
Loi relative au moyen d'instruments de transfert électronique de fonds													
V. Electronic commerce: 5. Publicity on Internet													
Arrêté royal - l'envoi de publicités par courrier électronique							Directive 97/55/EC concerning Misleading Advertising		Act: imposing limitations and penalties on the transmission of unsolicited commercial electronic mail via the Internet				
							Communication from the Commission of 22 January 2004 on Unsolicited Commercial Communications or 'Spam'						
V. Electronic commerce: 6. Domain names/Internet													
							Directive 98/34/EC for the Provision of Information in the field of Technical Standards and Regulations					Recommendation on the Legal Value of Computer Records (1985)	Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux
							Decision No. 854/2005/EC establishing a Multi-annual Community Programme on Promoting Safer Use of the Internet						Directive of 14 May 1991 on the Legal Protection of Computer Programs (91/250/EEC)
													Council Resolution of 21 November 1996 on New Policy - Priorities regarding the Information Society (96/C 376/01)
VI. Cyber crimes: 1-Internet crimes													
Loi fixant les signatures électroniques et les services de certification	Code Pénal Articles 226-16 à 24	Federal Data Protection Act of 20 December 1990			Ordonnance sur la conduite de la guerre électronique	Computer misuse Act 1990	Recommendation No. (95) 1995 concerning problems of criminal procedural law connected with information technology	Criminal Code of Canada	Computer Crime and Electronic Evidence			Manual on the prevention and control of computer-related crime	Convention on Cyber crime (Budapest, 23 November 2001)
									USA Computer Crimes Procedural				Additional Protocol to the Convention

EU countries							European Council	North America		ASEAN		UN/UNICTRAL	Conventions
Belgium	France	Germany	Luxemburg	Sweden	Switzerland	United Kingdom	EC	Canada	United States of America	Malaysia	Singapore		
									Acts 18 U.S.C. 2510 2511 to 2522, 2705 2701 2702 2703, 2704, 2711, 2000, 1029, 1030				on Cyber Crime concerning the criminalisation and xenophobic nature committed through computer systems, (Strasbourg, 28 January .2003)
									USC Tit. 15 Chap. 103 Sec. 7704. Controlling the assault of non-solicited pornography & Marketing				Bucharest Declaration on Combating Counterfeiting and Piracy (12 July 2006)
									Act - imposing limitations and penalties on the transmission of unsolicited commercial electronic mail via the Internet				
VI. Cyber crimes: 2. Computer crimes													
		Federal Data Protection Act of 20 December 1990				Computer misuse Act 1990	Recommendation No (89) 9 on computer-related crime	Criminal Code of Canada		Computer Crimes Act 1997		Manual on the prevention and control of computer-related crime	IT Security and Crime Prevention Methods (Interpol)
							Recommendation No. 95/1995 concerning problems of Criminal Procedural Law connected with Information Technology		Computer Crimes Acts 18 U.S.C. 1029, 1030, 1362, 1341, 1343, 2510, 2511, 2512 47 U.S.C.553, 605				Council Framework Decision on Attacks against Information Systems
							Directive 96/9/EC on the Legal Protection of Databases.		Computer Security Act of 1987				
							Council Framework Decision 2005/222/JHA on Attacks against Information Systems		Provisions of section 225; Cyber Security Enhancement Act				
									Computer Crime and Electronic Evidence				