Expert Meeting on

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

25-27 March 2015

Policy Note:

Development and Harmonization of Cyber Legislation in the Arab Region

By

UN-ESCWA

United Nations Economic and Social Commission for Western Asia

Policy Note

Development and Harmonization of Cyber Legislation in the Arab Region

ESCWA

United Nations Economic and Social Commission for Western Asia

Distr.
LIMITED
E/ESCWA/ICTD/2013/Technical Paper.2
4 July 2013
ENGLISH
ORIGINAL: ARABIC

ECONOMIC AND SOCIAL COMMISSION FOR WESTERN ASIA (ESCWA)

POLICY NOTE

DEVELOPMENT AND HARMONIZATION OF CYBER LEGISLATION IN THE ARAB REGION

United Nations
New York, 2013

13-0138

Acknowledgements

The present policy note was prepared on the basis of the studies and results of the regional project entitled "Regional harmonization of cyber legislation to promote the knowledge society in the Arab world", implemented by the Information and Communication Technology Division of the Economic and Social Commission for Western Asia (ESCWA) over the period 2009-2012.

Ms. Nibal Idlebi, Chief of the Information and Communication Technology Applications Section, prepared the present note in collaboration with Ms. Hania Dimassi, Section Research Assistant, with reference to a working paper on implementing ESCWA cyber legislation directives in the Arab region, prepared by Mr. Younes Arab, a cyber legislation legal expert and Head of the Arab Law Group; and a working paper on the legal reality of cyberspace, prepared by Mr. Abdulhay al-Sayed, an expert in cyber legislation and Managing Partner in Sayed and Sayed Law Firm.

CONTENTS

Introduction

Following the development of the digital age and efforts to build a modern knowledge society, information and communications technology has become the main driver behind the process of gathering, exchanging, storing and processing information, as well as a tool for generating knowledge, thus assisting in developing various economic and social sectors. This technology plays an important role in the Arab region by propelling sustainable development, providing new employment opportunities for young people and stimulating economic growth. Innovation also plays an ever-growing part in building a knowledge society; studies show that information and communications technology is the main engine of innovation in purely technological sectors and in other economic and social sectors.

The Internet is considered the largest information store in the knowledge society; it is also the principal tool for interaction between individuals and institutions; a platform for educational and scientific applications and for the provision of electronic government (e-government) services; and a trade tool. Statistics indicate that over a third of the world population use the Internet in their daily lives to carry out their work and various other activities. Improving access to the Internet has become a key factor in countries transitioning to a knowledge-based economy; they are competing in developing Internet infrastructure, especially broadband Internet. Despite the efforts of several Arab countries to improve access to information and communications technology, the digital divide, especially in terms of using and investing in such technologies, remains large between Arab countries and developed countries.

Stimulating the use of the Internet and its applications and electronic services in the Arab region requires an increase in confidence in cyberspace and its various applications. Cyberspace legal and organizational frameworks are the cornerstone for enhancing user confidence and guaranteeing their rights in their administrative, commercial and governmental undertakings, by creating a professional cyberspace image and assisting in making the information and communications technology sector independent, like other economic sectors. The majority of developed countries have recognized the need to enact cyber legislation and have updated cyberspace legal and organizational frameworks to meet contemporary requirements. Despite many developed countries, including Arab countries, attempting to enact cyber legislation, the process remains in its early stages. Moreover, all Arab countries lack a complete legislation package covering all cyberspace legal avenues.

Studies by the Economic and Social Commission for Western Asia (ESCWA) have highlighted the gap in cyber legislation between Arab countries and developed countries on the one hand, and between Arab countries themselves on the other hand. Given the comprehensive nature of cyberspace, which does not recognize borders or regions, international and regional coordination is extremely important for cyber legislation. The regional dimension of cyber legislation is of great significance to the Arab region, as cyber legislation coordination contributes to building an integrated Arab knowledge society to tackle information technology risks; stimulates electronic transactions and services between Arab countries; and contributes to protecting cyberspace intellectual property rights at the regional level.

The present policy note aims to clarify cyberspace legal frameworks and underscores the importance of cyber legislation in building an Arab knowledge society. It also sets out ESCWA research efforts and activities on developing and coordinating cyber legislation to strengthen regional integration. Moreover, it highlights the main challenges and obstacles that the Arab region faces in terms of enacting and implementing cyber legislation. It also contains a set of recommendations categorized by target or work scope. It should be noted that the recommendations were derived from ESCWA studies since 2007 and reflect the outcomes of negotiations held at conferences and workshops organized by ESCWA during the implementation of its project entitled “Regional harmonization of cyber legislation to promote the knowledge society in the Arab world”, unanimously approved by participating experts and decision makers.

I. IMPORTANCE OF CYBER LEGISLATION IN BUILDING A KNOWLEDGE SOCIETY

Cyberspace is considered as the bedrock of many developed economies. Undoubtedly, effective investment in cyberspace yields large economic and social benefits at the national level. Competitiveness at the regional and international levels requires a conducive environment, including developed and robust infrastructure; specialized human resources and expertise; the propagation of a culture of entrepreneurship and investment in innovation; and the development of comprehensive and integrated legal and regulatory cyberspace frameworks.

It should be noted that developments in communication media have broadened the scope of cyberspace, no longer limiting it to the Internet. It now covers all fixed and mobile communication methods and networks, including the Internet and its sites, services and applications. This highlights the importance of enacting and implementing cyber legislation to regulate the wide and swift spread of information and communication technology and its applications in economic, social, scientific, commercial and governmental sectors, as well as in various interactions among individuals and institutions. Such legislation will assist in making the information and communications technology sector independent and regulated like other sectors, such as transport, electricity and energy.

Cyber legislation is important for many reasons, including the need to develop a regulatory framework, standards and procedures to safeguard the information exchanged via the Internet, by electronic mail or other applications, and prohibit intermediaries from using such information without owner permission, misusing or misplacing it. To legitimize electronic transactions, develop checks and standards and protect Internet users, it is necessary to enact legislation on electronic trade and transactions to protect all stakeholders. Such laws are a vital factor in developing a conducive cyberenvironment; strengthening user confidence in cyberspace services and applications; and supporting and stimulating electronic trade at the regional and international levels, especially considering that companies use the Internet as an advertising tool and a platform for commercial transactions. Undoubtedly, investing in cyberspace will assist in stimulating national investment and attracting foreign investment in information and communication technology and other sectors that use such technology.

It is also necessary to regulate the use and storage of personal data, given that many e-government applications and financial and health services entail the storage of information belonging to individuals and institutions in databases and special systems. This information might be highly sensitive or private and therefore might need protection through laws that prohibit its misuse or unauthorized use.

The increasing number of applications and social networks and the growing number of Internet users from all social backgrounds have led to the misuse of cyberspace, including money scams, identity fraud and harassment. Such cybercrime has increased over the past few years. Several countries thus enacted cybercrime legislation as a deterrent for misuse and as a tool to pursue offenders and protect the victims' rights.

Lately, new nefarious uses of the Internet and cyberspace have been developed, known as cyberterrorism. There is an ongoing debate on the needed mechanisms to combat the phenomenon and pursue perpetrators. Cyberwarfare has also become a prominent topic, stimulating discussions on its nature and repercussions at the national and international levels, especially following cyberattacks on government, financial and military institutions in some countries. It later became apparent that other countries were involved in preparing and carrying out those attacks, which underscores the importance of cross-border cyber legislation given that cyberspace does not recognize geographical borders.

Cyber legislation can be categorized under the following four topics: laws aimed at protecting users by safeguarding privacy, personal data and user rights; criminal legislation on the misuse of cyberspace; laws to protect intellectual property rights regarding products, programmes and information posted on the Internet, in

accordance with country specificities and innovation stimulation; and laws aimed at regulating administrative and commercial transactions.

II. ESCWA PROJECT TO COORDINATE CYBER LEGISLATION IN THE ARAB REGION

Since 2007, ESCWA has prepared studies and organized activities to research cyber legislation and stimulate its development in the Arab region. The first study entitled "Models for cyber legislation in ESCWA member countries"[1] reviews the enactment of cyber legislation at the regional and international levels and compares the Arab region to other regions in that regard. The study highlights the cyber legislation gap between regions, especially between the Arab region and the European Union that has developed and implemented a number of guidelines and directives on cyberspace regulation. In 2008, ESCWA issued a template[2] setting out the key elements of each cyberspace law to assist countries in enacting cyber legislation and in evaluating existing laws and their shortfalls. ESCWA applied the template to several Arab countries and published tables for member States outlining their national laws on the basis of the template.

It should be noted that ESCWA discussed the above-mentioned study and template at several meetings and workshops with regional cyber legislation experts. In the light of their repeated recommendations on the need to undertake a regional project to coordinate laws at the regional level and tackle their shortfalls, ESCWA launched a project entitled "Regional harmonization of cyber legislation to promote the knowledge society in the Arab world", which began in 2009 and was completed in 2012.[3] The project aimed to strengthen and coordinate cyber legislation in the Arab region to establish a solid and sustainable information and communications technology sector by developing appropriate legal frameworks.

The project led to the implementation of several activities with various outcomes, including the document entitled "ESCWA cyber legislation directives"[4] designed to assist Arab States in enacting national cyber legislation and developing the basic building blocks for regional integration through cyber legislation coordination, so as to build an Arab knowledge society. Those directives cover the following six core themes for cyberspace regulation that can either be used as standalone laws by theme or as one comprehensive law: electronic communication and freedom of expression; electronic transactions and signatures; electronic trade and consumer protection; personal data processing; cybercrime; and intellectual property rights in cyberspace. Each theme includes a background research paper containing guidance, followed by an introduction and a review of the provisions of the laws. The directives not only aim to review legal texts, but also to facilitate legal research and clarify legal documents.

ESCWA worked in collaboration with a group of distinguished legal experts, specializing in information and communications technology, to prepare and draft the directives. It also held an expert group meeting[5] to review and discuss the directives prior to preparing their final draft. It should be noted that the process was undertaken in the light of extensive studies on cyber legislation enactment in the Arab region, and took into account regional and international experiences in the field, especially those of the European Union.

---

[1] ESCWA, 2007.

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

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

[4] http://isper.escwa.un.org/Portals/0/Cyber%20Legislation/Regional%20Harmonisation%20Project/Directives/Directives-Full.pdf (Arabic only).

[5] Expert Group Meeting on the Regional Harmonization of Cyber legislation in the Arab Region (Beirut, 16/17 February 2011). www.escwa.un.org/information/meetingdetails.asp?referenceNum=1427E.

Under the same project, ESCWA organized regional awareness-raising workshops on the ESCWA cyber legislation directives and on promoting their use in the region, and provided training on the mechanisms for their implementation. It collaborated with governmental and non-governmental national and regional bodies to organize national workshops for legal personnel, including lawyers, judges and legal experts specializing in information and communications technology. Decision-makers from information and communications technology ministries and entities and justice ministries participated in the workshops, as well as experts and specialists from the private sector and regional and international organizations.

ESCWA, at the request of several member States, provided advisory services to countries on applying the ESCWA cyber legislation directives at the national level. The aim of such services was to evaluate the gap between existing national laws and the ESCWA directives, and to review draft cyber legislation prepared by countries on the basis of the ESCWA directives and in accordance with national legal frameworks. Draft bills and national training workshops were also proposed for some countries.

The project concluded with a seminar on the legal and regulatory requirements for building a sustainable knowledge society in the Arab region,[6] which reviewed a proposed regional framework for action to implement the ESCWA cyber legislation directives in the Arab region; and determine the role of countries in enacting cyber legislation at the national level, and the role of the League of Arab States and regional organizations in coordinating such legislation at the regional level. The seminar included presentations and discussions on future regional and international directions in the field and the challenges posed by new technologies, including mobile applications and cloud computing.

III. CYBER LEGISLATION CHALLENGES IN THE ARAB REGION

ESCWA studies and expert group discussions have indicated several challenges and obstacles facing Arab States in terms of cyber legislation, which affect decision-makers, parliamentarians, legal personnel, government institutions, the private sector, civil society and individuals. These challenges have been divided into the following categories: challenges related to the complexity of cyber legislation references; challenges linked to drafting and enacting laws at the national level; and challenges related to implementing cyber legislation.

A. ABSENCE OF STANDARDIZED REFERENCES FOR CYBERSPACE REGULATORY AND LEGAL ISSUES

The absence of standardized references for cyberspace regulatory and legal issues[7] and the lack of coordination among numerous, sometimes overlapping, references that can sometimes go beyond their legislative remit, form the main obstacle to legislation drafting and implementation in Arab countries. The absence of a single body that monitors the legal and regulatory environment of cyberspace in a country negatively affects the quality and comprehensiveness of cyber legislation frameworks. To resolve this issue, legislation within countries must be harmonized in terms of concepts, terminology and responsibilities, among other things, to ensure quality, effectiveness and comprehensiveness upon implementing the ESCWA directives.

A unified framework would allow for the serious regulation of cyberspace in a way that protects the rights and interests of digital users; and allows countries to realize the visions contained in information technology strategies while ensuring their effective interaction with knowledge-based economies.

[6] The seminar was held at the United Nations House in Beirut, on 19 and 20 December 2012. www.escwa.un.org/information/meetingdetails.asp?referenceNum=2002E.

[7] Arab, 2012.

B. FORMULATING AND ENACTING CYBER LEGISLATION AT THE NATIONAL LEVEL

All Arab States have included cyber legislation as a key theme in their national strategies on information and communications technology, in recognition of its importance in building a knowledge society and a knowledge-based economy. Cyber legislation is also prominent in regional strategies and action plans that aim to secure a conducive regulatory environment for an effective use of cyberspace, such as the regional action plans for building a knowledge society (prepared by ESCWA in 2005);[8] and the Arab Information and Communication Technology Strategy (2007-2012),[9] given its importance in achieving the first strategic goal on enhancing confidence and security in the use of information and communication technology and its applications. The Arab Information and Communication Technology Strategy fundamentally focuses on safeguarding privacy, personal data and intellectual property rights in the digital realm, and on combating all forms of cybercrime.

Despite the above, studies have shown that the majority of Arab countries suffer from cyber legislation gaps. This is a modern problem linked to rapid changes and developments in information and communications technology, and the late recognition of the importance of knowledge societies and economies that were not provided with suitable environments for development in several Arab countries. Moreover, the slowness in formulating and enacting legislation, especially over the past two years because of the unrest in the Arab region, and the overlap of certain existing cyberlaws—especially laws on telecommunication sector regulation that have existed for decades, making their amendment to include provisions on communication via the Internet and electronic transactions relatively complicated—present added difficulties for countries. The same applies to criminal and penal laws, given that including provisions or a specific law on cybercrime requires a concerted effort to determine the nature of cybercrimes, how to prove that they have occured and decide how they should be punished, in accordance with national laws. Some countries have tried to bridge this legislative gap by enacting laws on specific issues, such as electronic transactions, by quoting foreign laws or referring to international treaties.

1. *Need for varied expertise*

The variety and complexity of cyber legislation, especially its technical and legislative aspects, means that varied expertise is required in national committees responsible for drafting such legislation. Legal, methodological and technical discussions among experts are also necessary to ensure that laws are issued complete and free from specific details on communication and information technology because of the continuous changes and rapid developments in the field. Given the numerous cyber legislation stakeholders in the Arab region, drafting committees should include representatives of all stakeholders to ensure that all perspectives are considered.

Drafting committees should also include legal and legislative experts and information and communication specialists, given that the enactment of certain laws requires detailed knowledge of specific information and communication issues, such as encoding for electronic signature laws.

Moreover, drafting national cyber legislation requires knowledge of other countries' cyber legislation and experiences, and awareness of existing international legislation, given the comprehensive nature of cyberspace and the importance of regional and international cooperation in the field. Referring to the experiences of other countries is essential, as is ensuring that cyber legislation meets national needs and is consistent with countries' legal, social and jurisprudential frameworks.

Enacting cyber legislation requires a clear national approach, involving all relevant parties, bodies and ministries. The following attitudes pose obstacles to cyber legislation formulation: leaving legislation

[8] www.escwa.un.org/divisions/div_editor/Download.asp?table_name=divisions_other_ar&field_name=ID&FileID=251.

[9] isper.escwa.un.org/RegionalActionPlans/ArabICTStrategy/StrategyDocument/tabid/70/language/en-US/Default.aspx.

development to one party; violating relevant constitutional rules; and claiming that the legislative authority is the only body capable of understanding all the technical and legal aspects of enacting cyber legislation.

2. *Categorizing cyber legislation issues*

Several approaches have been adopted to bridge the cyber legislation gap in Arab countries. Some countries amended existing laws by adding provisions on cyberspace, such as integrating cybercrime in criminal and penal laws, or amending consumer protection laws to include Internet transactions. It became apparent that this approach was not sufficient because it only applied to certain matters rather than covering the cyberspace issue in its entirety. It is no longer widely used because of its lack of comprehensiveness and because of the constant developments in information and communication technology and its various applications.

A more widespread approach is the enactment of several laws, each covering one or more cyber legislation issues, such as electronic signatures, electronic transactions and cybercrime. Many Arab States have adopted this approach because it is simpler than enacting a single law that covers all cyberspace issues. Nevertheless, this approach results in weak coordination and compatibility between various cyberlaws; an unmanageable number of references; weak understanding of issues and terminology; and an inability to view cyberspace as a single milieu. It should be noted that several Arab States incorporated many issues in one law, such as including e-transaction and e-commerce in the same law or placing e-signature under e-commerce. Other countries have integrated cybercrime laws in legislation on e-commerce and e-transaction.

Experts recommend the comprehensive approach of enacting one law covering all cyberspace issues, as is the case in Malaysia and South Africa. Such a law can be designated as the Law on Information and Communication Technology; Law on Information Technology; or Cyberlaw (as in Malaysia). Despite the difficulties of this approach, it ensures full coverage of all cyberspace issues and assists in unifying operational and monitoring procedures, especially if a single party is selected to monitor its implementation. It also guarantees integrated and consistent legal solutions and rulings under one law. For example, the new Lebanese law on information technology covers several issues, including the following: e-signature, e-transaction, cybercrime and personal data protection, making it an almost fully comprehensive cyberspace law. ESCWA has widely adopted this approach by developing an integrated set of directives covering six cyberspace issues, hoping that these directives will be adopted in the Arab region to enhance legislation coordination between countries and provide opportunities for regional and international exchange and interaction.

3. *Mechanisms for drafting and endorsing cyber legislation*

The process of drafting and endorsing legislation is extremely slow for several reasons in the Arab region, including complex hierarchies and political intervention that sometimes plays a role in bill delays. The social unrest that occurred in some countries in 2011 played a part in postponing or stopping legislative processes at all stages, including drafting, draft bill reviews and adoption by parliaments, many of which were suspended.

ESCWA studies show that many Arab States use translated foreign laws, resulting in cyber legislation that is incompatible with the societies that it aims to regulate, when it should reflect their reality. It is often felt that cyber legislation is unsuited to the legal framework under which it has been placed, because it tackles modern issues or because laws have been badly translated and are irreconcilable with existing national legislation. Past experiences show the difficulties of translating technical foreign texts, and studies indicate that authorities in Arab countries strive to alter legislation following translation in the name of national specificities, causing issues of containment, surveillance and punishment to override the principle of freedom of communication on the Internet.

ESCWA studies also show that some countries' concern with a certain legislative issue might not stem from national needs but rather from external influences, such as the ratification of international treaties. It has been noted that Arab States rush to comply with such treaties regardless of national priorities.

C. Enacting cyber legislation

Law enactment is linked to the availability of necessary regulations, procedural decisions and regulatory instruments. Their absence poses a challenge to enacting and implementing legislation. Some Arab States have endorsed laws on electronic commerce and transactions, but such services are rarely used because of weak regulations and procedures, leading to low enactment of relevant legislation. The following are the principal obstacles to enacting and implementing cyber legislation:

(a) Institutional structures: the absence, weakness or ineffectiveness of measures for the establishment or selection of regulatory, operational and supervisory bodies concerned with cyber legislation is one of the main obstacles to its implementation. Experiences in the Arab region have highlighted the weakness of institutional structures, which are completely absent in some countries. Some bodies concerned with legislation implementation are not assigned basic tasks that similar bodies in other regions are responsible for, thus hampering the process;

(b) Regional cooperation and coordination: the absence or weakness of regional and international coordination on certain technical issues related to cyber legislation, especially those concerned with cybercrime, impede the implementation of such legislation at the national level;

(c) Judicial police: the lack of judicial police systems, including specialized personnel and financial and technical requirements, reduces the effectiveness of legislation. Practical implementation of legislation requires specialized equipment; competent personnel who are kept up to date with the latest technologies; and mechanisms to monitor, limit and investigate breaches and infringements before referring them to the courts for their consideration;

(d) Public prosecutors and the judiciary: the weakness or absence of training for public prosecutors and the judiciary on cyber legislation issues; the lack of specialized courts; and the weakness of technical offices regarding the analysis, documentation and publication of rulings and outcomes for researchers and study centres present additional obstacles to the enactment and implementation of cyber legislation in practice.

IV. RECOMMENDATIONS

While implementing the project entitled "Regional harmonization of cyber legislation to promote the knowledge society in the Arab world", ESCWA collaborated with several experts and regional organizations concerned with building the information society and involved stakeholders concerned with enacting cyber legislation in the Arab region. The meetings held on the project resulted in the development and discussion of a set of recommendations, divided into the following five categories: recommendations to Governments on drafting and completing cyber legislation; recommendations on the legislative process; recommendations on implementing cyber legislation; recommendations on the regional dimension of cyber legislation; and recommendations on awareness-raising and training.

A. Recommendations for governments on drafting and updating cyber legislation

It is highly important to develop and update comprehensive cyber legislation that covers all issues related to cyberspace, protects user rights and builds confidence in cyberspace and its applications, in accordance with the requirements of the digital realm and its applications. The best way to establish effective legislative and regulatory frameworks for cyberspace in the Arab region is firstly to develop a

comprehensive and specialized supervisory framework, founded on a strategy with clear goals and mechanisms. Countries have the following two options to tackle challenges at the national level: endorsing the status quo and developing it without undertaking fundamental changes; or completely reforming the system, which is undoubtedly the better and more effective option.

Countries can adopt the following three approaches to face obstacles and challenges at the national level related to enacting cyber legislation, especially the challenge of numerous cyberspace parties and entities and diverging outcomes as a result:

(a) First approach: establishing one body tasked with updating cyber legislation frameworks by evaluating existing laws, proposing amendments and measures to cover shortfalls and ensuring coordination among them. The effectiveness of this approach depends on developing a single coordinated law on cyberspace as a whole or one that covers the largest possible number of cyberspace issues; on establishing a single body responsible for cyberspace, policy and legislation; and greatly reducing regulatory and operational frameworks, provided that they remain able to carry out regulatory responsibilities. This approach invariably requires fundamental change. The best option is to develop a law that can be designated as "Law on Information and Communication Technology" or "Law of Cyberspace";

(b) Second approach: developing a single coordination framework that includes all parties and bodies concerned with cyber legislation, covering its shortfalls, coordinating relevant legislation and implementing its projects. This approach supports the existence of various legislative bodies, rearranged under a coordination framework, rather than a single supervisory or operational framework, to enact legislation that practically and procedurally covers all cyberspace branches and issues. The approach does not result in single law on cyberspace but rather in a coordinated set of laws, which might suit the Arab region;

(c) Third approach: this approach could be imposed by the absence of political decision in the cyberspace coordination framework, or lack of confidence in the capabilities of existing frameworks to achieve desired goals. To avoid this, state legislative authorities should evaluate existing cyber legislation at the national level and propose amendments, new measures and plans to implement outcomes. This process should be carried out by experts and reviewed by all relevant bodies for their contributions. The outcome should then be submitted to lawmakers for their approval.

Regardless of the adopted approach, drafting legislation requires the following:

(a) Evaluation by legislative authorities of existing cyber legislation at the national level, using detailed research and studies to determine shortfalls and best mechanisms to find and implement solutions. This process should be undertaken by an expert group and should involve relevant ministries and bodies for the review and approval of the evaluation;

(b) Establishment of specialized committees to draft cyber legislation, comprising experts in law and in information and communications technology. They should also include relevant civil society and private sector representatives;

(c) Reference to regional and international agreements on cyber legislation to ensure compliance of national legislation. Countries should accede to such agreements if they meet national needs and priorities. Reference should also be made to the ESCWA cyber legislation directives that cover all cyberspace issues, including the right to access information, which is vital to building a knowledge society.

B. RECOMMENDATIONS ON THE LEGISLATIVE PROCESS[10]

Enacting cyber legislation requires varied expertise, especially in law and in information and communications technology. It should also take into account the needs and requirements of the public and private sectors and civil society institutions, including specialized associations and unions. It is therefore necessary to create the right conditions to ensure that legislation reflects the needs of the societies that it is regulating, rather than mirroring foreign legislation that is not compatible with the Arab region. Given the novelty of cyber legislation in Arab countries and lack of experience in the field, the following recommendations have been proposed:

(a) Enhancing the transparency of the legislative process when drafting, discussing and approving legislation by broadening the membership of legislative committees to include all relevant stakeholders, such as ministries, government institutions, civil society organizations, internet users and private companies, including Internet providers. Legislative committees should therefore not only comprise experts and external consultants;

(b) Comprehensively and clearly compiling and storing all legislative committee deliberations in a searchable manner to assist in implementing legislative texts following their approval;

(c) Developing field research methods during the legislative process to record good Internet user behavioural, transactional, contractual and procedural patterns and their perceptions on how to improve cyberspace,[11] so as to benefit from them during the legislative process. Infringements and misuse should also be recorded to facilitate the enactment of legislation to tackle them. Developing field research methods requires the assistance of sociologists who use observation and field research tools, including statistics, opinion polls and personal and group interviews;[12]

(d) Coordinating legislative texts within countries to avoid potential overlap or contradiction between cyber legislation and other existing laws. Although e-transactions occur electronically at a distance, legislation governing them could reiterate existing general contract regulations,[13] among other things. Contradictions in legislative texts could lead to problems in their implementation, which might render them ineffective.[14] It is therefore essential to issue a list under each new legislative article, indicating all existing legal texts affected by new legislation (amending or abolishing them);

(e) Encouraging the provision of explanatory notes that include official comments on legislative articles, following the completion of legislative deliberations and the issuance of legislation by relevant parties. Notes should also contain a summary of deliberations by drafting committees; a commentary on each legislative article, including a detailed report on the legislative policy employed in the text; the interests that the text aims to maintain or rebalance; and the scope of its implementation;

(f) Focusing on jurisprudence; researching it and conducting studies to compare jurisprudence in Arab countries with that of selected developed countries, given its importance in law; and establishing specialized research groups in cyberjurisprudence to assist in publishing legal precedent and commenting thereon;

---

[10] This section is based on Al-Sayed, 2011.

[11] Dupret, 2006, p. 173.

[12] Guibentif, 2002, pp. 311-339.

[13] Hijazi, 2007, p. 331 onwards.

[14] ESCWA, 2009, pp. 11-14.

(g) Presenting first drafts of cyber legislation for public consideration and encouraging public debate thereon through various electronic methods that allow for the exchange of comments and contributions on draft legislation, or through national workshops and seminars involving all stakeholders to ensure a balanced and effective public debate;

(h) Encouraging non-governmental organizations involved in legislation to establish working groups that assist in urging Governments and legislative councils to enact cyber legislation.

C. RECOMMENDATIONS ON IMPLEMENTING CYBER LEGISLATION

Recommendations on implementing cyber legislation focus on key mechanisms for its implementation after its approval, and on its compatibility with the societies that it is regulating:

(a) Urging Governments to develop regulations and operational procedures for cyber legislation, establishing the organizational structures for its implementation and allocating the required funding. Either one of the following two options can be adopted to determine the organizational structures needed for implementing cyber legislation:

(i) Establishing a single high commission responsible for cyber legislation and its regulation, through a special legislative measure that takes into account existing organizational structures, guarantees coordination among them and proposes amendments to them. This is considered the best and most comprehensive option, but requires fundamental changes that are difficult to achieve in some countries;

(ii) Developing a coordination framework among government bodies to avoid duplication in the drafting and implementation of legislation and overlap in addressing its shortfalls. This option allows for multiple bodies responsible for cyber legislation but requires an official decision to guarantee their commitment, determine their remit and responsibilities and the coordination mechanisms for joint projects and programmes;

(b) Preparing studies on the economic feasibility of providing funding for legislative organizational structures. Providing such resources is a key issue being researched by relevant constitutional bodies in all Arab countries, including the possibility of organizational structures self-funding by using licensing fees and grants, among other sources; by relying on allocations from government budgets; or combining the two. This also raises the issue of financial resources: should such structures keep all or part of the funding or should they transfer it to state treasuries? How will expenses be covered when there is a budget deficit?

(c) Training suitable operational and legal personnel by raising awareness among personnel responsible for implementing legislation, using global good practices in the cyberspace field and existing legislative rules and regulations, so as to increase the efficiency of legislation in the societies it aims to regulate;[15]

(d) Developing legislative solutions that are compatible with the reality on the ground and societal views, after analysing the nature and patterns of societal relationships, so as to ensure more effective implementation of legislation;

(e) Allocating financial and human resources for field research to record and categorize existing practices at the national level in various cyberspace fields, allowing legislators to monitor the interaction of societies with legislation and determine the required legislative procedures to handle existing legal realities.

[15] Harb and others, 2008, p. 22.

D. RECOMMENDATIONS ON THE REGIONAL DIMENSION

The importance of regional cooperation and coordination at the Arab and international levels is highlighted in legislative processes and legislation implementation, given the comprehensive nature of cyberspace and the importance of regional coordination to ensure the consistency of cyber legislation and drive the regional integration process forward to build an Arab information society.

Regional coordination of cyber legislation facilitates the recognition of digital evidence at the regional level; stimulates electronic transactions among Arab countries, especially commercial transactions; and greatly contributes to combating cybercrime and monitoring its effects at the regional level. It should be noted that adopting intellectual property laws for cyberspace that are consistent with Arab countries' economic, social and cultural situations greatly contributes to building a regional knowledge-based economy. This highlights the role of regional organizations in increasing coordination efforts, and regional and international cooperation, and striving to ensure the consistency of cyber legislation in the Arab region.

1. *Role of the League of Arab States*

The League of Arab States plays a fundamental role in developing and endorsing regional treaties; providing political and strategic support to them; adopting Arab model laws for cyber legislation; and ensuring coordination and cooperation between Arab States in implementing treaties on cyber legislation. The adoption of legal treaties is generally undertaken by relevant ministerial councils. With regard to cyber legislation, coordination is required between certain ministerial councils, especially communication, justice and interior affairs councils, to cover all cyber legislation issues. It is also important to develop a single administrative framework within the League of Arab States to consider all cyber legislation issues.

The main justifications for organizational and legislative cooperation, coordination and interaction regarding cyber legislation relate to the comprehensive nature of cyberspace. For example, the efficiency of judicial and investigative cooperation between Arab countries on cross-border cybercrime would be enhanced through unanimously approved legislative solutions and action plans to combat cybercrime, and would guarantee consistency between regulations and existing standards and measures in all Arab countries. It should be recognized that Arab countries cannot secure a place in the electronic market if they do not cooperate to create a powerful Arab regional bloc in cyberspace.

Arab coordination on cyberspace issues is necessary for Arab countries to cement their presence in cyberspace in the future. Large entities have a more effective presence in cyberspace and small entities cannot achieve such an effective presence, regardless of their efforts, solutions or measures.

It should be noted that the League of Arab States issued the following laws for the Arab region: an Arab guidance law on modern techniques; an Arab draft convention to combat cybercrime; and an Arab guidance law on electronic transactions and commerce. However, these laws do not cover all cyberspace issues. The Economic Commission for Africa (ECA) is preparing a draft African convention that includes several Arab countries in North Africa, so as to build confidence in cyberspace. It covers electronic transaction regulation, personal data protection and combating cybercrime.

On the basis of the above and of regional experiences regarding cyber legislation, and after the establishment of a single coordination framework for relevant bodies, the following solutions to cyberspace issues could be implemented in coordination with the League of Arab States:

(a) Adopting the ESCWA cyber legislation directives as a model for the region;

(b) Developing a comprehensive Arab convention on all cyberspace issues in accordance with the ESCWA cyber legislation directives;

(c) Re-evaluating operator communication plans and regulatory measures in accordance with international standards, especially those of the International Telecommunication Union (ITU) and its bodies;

(d) Focusing on developing conventions that ensure judicial and investigative cooperation to meet cyberspace requirements and the substantive, legal and procedural regulations endorsed by Arab States;

(e) Undertaking the knowledge exchange project and publishing the outcomes of implementing all branches of cyber legislation and its challenges in the Arab region;

(f) Cooperating with regional and international organizations to organize awareness-raising programmes on cyber legislation;

(g) Supporting efforts to standardize Arabic cyber legislation terminology and launching a project to develop an Arabic thesaurus on cyberspace databases.

2. *Role of international and regional organizations*

Regional and international organizations concerned with building a knowledge society and a knowledge-based economy in the Arab region support the League of Arab States in developing a legal and regulatory framework for the Arab region. Key organizations include ESCWA, the Office for North Africa of ECA, the United Nations Office on Drugs and Crime, the ITU Arab Regional Office, the Arab Administrative Development Organization and the Arab Information and Communication Technologies Organization. Given the number of these organizations, coordination, cooperation and information exchange among them is vital to achieving better results at the regional level.

The following are some of the tasks could be undertaken in coordination with regional and international organizations:

(a) Informing Arab legislative bodies in Arab countries of the legal challenges of cyberspace and the necessary measures to tackle them in accordance with minimum national, regional and international agreed standards;

(b) Providing tools to objectively evaluate cyber legislation and its practical applications in development projects;

(c) Assisting Arab States in tackling shortfalls and overcoming obstacles in cyber legislation regulatory and legislative frameworks, or developing new comprehensive frameworks, with reference to advanced experiences that have proved their effectiveness in the field;

(d) Activating regional cooperation and coordination and developing a legislative and regulatory cyberspace framework at the regional level, which is comprehensive, effective, implementable and consistent with best international standards compatible with the specificities of Arab legal frameworks, so as to enhance the digital realm and strengthen the Arab position in cyberspace;

(e) Organizing, participating in and monitoring training programmes on implementing cyber legislation measures and evaluating performance in the field;

(f) Launching or supporting the implementation of relevant regional projects and improving legal performance and knowledge requirements for cyberspace;

(g) Supporting efforts to standardize Arabic terminology in the information and communications technology field, especially concerning cyber legislation; cooperating with Arab language academies to approve standardized terminology; and developing an Arabic thesaurus on cyberspace databases.

ESCWA, through its project on regional harmonization of cyber legislation to promote the knowledge society in the Arab world, implemented several of the above-mentioned activities. The ESCWA cyber legislation directives are being widely employed in the development of national laws and their coordination at the regional level, thus enhancing regional integration to build a knowledge society and a knowledge-based economy.

ESCWA will continue to support Arab States in addressing cyber legislation gaps by offering advisory services and organizing national and regional workshops to build capacities in the field. ESCWA will also strive to ensure regional coordination and integration in the field and will provide platforms for the exchange of experience between Arab countries and through which they would also benefit from the expertise of other countries and regions. Moreover, ESCWA will collaborate with the international community to take into account Arab country specificities when developing legal and regulatory cyberspace frameworks. It will also continue its work in the field of legal and regulatory cyberspace framework policy, focusing on combating all forms of cybercrime.

At this stage, following the success of the ESCWA project, it is important to coordinate between ESCWA and the League of Arab States through the Arab information and communication ministerial councils and the justice ministerial councils; and to formulate an Arab convention covering all cyber legislation issues to protect cyberspace and support its applications and electronic services.

E. Recommendations on awareness-raising and training

Awareness-raising is an important issue in many fields. To successfully implement cyber legislation and build an integrated system for it, including institutions and personnel, special attention should be given to training and awareness-raising at all levels, to ensure the understanding and awareness of cyber legislation details and its implementation mechanisms. It is therefore recommended to organize a variety of national workshops and seminars under a comprehensive national project, rather than just random activities, as follows:

(a) Organizing workshops for legislatures and parliamentarians on the importance of cyber legislation for building confidence in cyberspace and electronic services and for protecting users;

(b) Developing a specialized training programme for judges and lawyers on drafting laws that meet cyberspace requirements;

(c) Holding national workshops for technicians, union members, security personnel and judicial officers on cyber legislation and its implementation;

(d) Holding national and regional expert group meetings on cyber legislation to exchange new experiences and expertise in the field;

(e) Implementing training programmes for judicial officers and bodies using specialized personnel and necessary technical methods;

(f) Developing awareness-raising programmes targeting all social groups on cyber legislation and its importance in protecting Internet users;

(g) Developing university programmes by including cyber legislation topics in the curricula of information and communications technology academies; specialized and advanced programmes; law faculties; and advanced law programmes, and holding training sessions on the issue during the first stages of legal schooling.

REFERENCES

Al-Sayed, Abdulhay (2011). *Recommendations on the Legal Reality of Cyber legislation.* Available from http://isper.escwa.un.org/Portals/0/Cyber%20Legislation/Regional%20Harmonisation%20Project/Studies/StatusCLArabRegion.pdf (Arabic only).

Arab, Younes (2012). *Implementing the ESCWA Cyber legislation Directives in the Arab Region*. http://isper.escwa.un.org/Portals/0/Cyber%20Legislation/Regional%20Harmonisation%20Project/Directives/Application%20of%20Directives.pdf (Arabic only).

Dupret, Baudoin (2006). *Droit et Sciences Sociales.* Paris: Armand Colin.

Economic and Social Commission for Western Asia (ESCWA) (2007). *Models for Cyber legislation in ESCWA Member Countries.* Available from www.escwa.un.org/information/publications/edit/upload/ictd-07-8-e.pdf.

ESCWA (2009). *Review of Information and Communications Technology and Development,* Issue 11. Available from http://isper.escwa.un.org/Portals/0/Cyber%20Legislation/Documents/ICT%20Review%2011%20(Ar).pdf (Arabic only).

ESCWA (2012). ESCWA Cyber legislation Directives. Available from http://isper.escwa.un.org/Portals/0/Cyber%20Legislation/Regional%20Harmonisation%20Project/Directives/Directives-Full.pdf (Arabic only).

Guibentif, Pierre (2002). "Questions de méthode en sociologie du droit. A propos de l'entretien en profondeur", in *Pour un droit pluriel. Etudes offertes au professeur Jean-François Perrin.* Bâle: Helbing and Lichtenhahn.

Harb, Wassim and others. (2008). *Models for Cyber legislation in ESCWA Member Countries*. Available from www.escwa.un.org/information/publications/edit/upload/ictd-07-8-e.pdf.

Hijazi, Abdulfatah (2007). *Legal Framework for Electronic Signatures.* Mahalla al-Kubra, (Arabic only).

United Nations House, Riad El Solh Square
P.O. Box: 11-8575, Beirut, LEBANON
Tel.: +961 1 981301; Fax: +961 1 981510
www.escwa.un.org

Printed at ESCWA, Beirut

E/ESCWA/ICTD/2013/Technical Paper.2
United Nations Publication
13-0138 – November 2014