Distr.: General

E/ECA/CODIST/1/15
26 March 2009

UNITED NATIONS
ECONOMIC AND SOCIAL COUNCIL

Original: English

ECONOMIC COMMISSION FOR AFRICA

First Session of the Committee on
Development Information, Science and Technology (CODIST-I)

Addis Ababa, Ethiopia
28 April – 01 May 2009

LEGAL AND REGULATORY FRAMEWORKS FOR THE KNOWLEDGE ECONOMY

CONCEPT PAPER

By Angeline Vere

I. INTRODUCTION

1. Over the years, there has been a paradigm shift in what constitutes the primary wealth-creating assets. In the sixteenth century, land and labour were the main means of production. The eighteenth century saw the transition of the global economy to an industrial focus where labour and capital became the fundamental wealth creation components. The twentieth century gave birth to information communication technologies which are knowledge driven. The information age began in the 1960s when the majority of workers were involved in the creation, distribution and application of information.1

2. Information and knowledge became a basic form of capital, replacing labour and energy (which was physically based). "The balance between knowledge and resources has shifted so far towards knowledge that it has become, perhaps, the most important factor determining the standard of living – more than tools and more than labour. Today's most technologically advanced economies are truly "knowledge-based"2. The basic principle of the knowledge economy is that economic growth is driven by the accumulation of knowledge. New standards of speed, efficiency and accuracy of communication have become the new tools for boosting productivity.

3. An enabling environment which allows and encourages creation of a knowledge economy is of paramount importance. Some components of an appropriate enabling environment include:

- Ensuring that the playing field allows for healthy competition in the ICT sector;
- Developing financial systems to mobilize capital to its most productive uses;
- Adoption of an appropriate legal and regulatory framework through introduction of a whole legal system supportive and free from legal barriers for the development of a knowledge economy; and
- Creation of an environment which offers basic assurances such as security, integrity, authenticity, confidentiality and data protection and privacy.

4. An appropriate legal and regulatory environment ensures that there are set rules and regulations which allow the ICT sector to be more competitive, thus allowing the economy to grow. It has been noted that there is a core relationship between the level of attainment of a knowledge economy and the inflow of financial investments. Countries that have advanced economies such as Australia, Germany, Japan, United Kingdom and the United States of America have all embraced e-commerce activities as a way of life and have enacted cyber legislation to regulate e-commerce activities. African countries aspire to attract financial investment to boost economic growth and should therefore embrace this trend towards creation of a knowledge economy. However, Africa is lagging behind and there is fear that it will be excluded from the digital revolution. The continent faces a number of challenges such as lack of technologically advanced telecommunications infrastructure, lack of legal and regulatory frameworks supportive of ICT developments and the high rate of illiteracy.

5. In recognition of these challenges, the Economic Commission for Africa (ECA) launched the African Information Society Initiative (AISI) in May 1996. The ECA vision is to

[1] James A. Senn, Information Technology in Business, Prentice Hall, Inc 1995.
[2] World Report 1999.

assist African countries in establishing a conducive environment in which knowledge is seen as a vital tool for economic growth and bridges the digital divide between Africa and the rest of the world. AISI provides the road map to guide African countries in addressing the challenges of emerging globalization and the information age by developing and implementing National Information and Communication Infrastructure (NICI) policies and plans.

6. In this context, this concept paper will analyse the development of e-commerce legal and regulatory frameworks which is an essential element in creation of an enabling environment for the knowledge economy. The paper focuses on the following components: the current status of cyber laws in Africa; legal issues to be covered by such laws; existing templates to be used; highlights of best practices; and what is being done at the level of the regional economic communities (RECs) to ensure that member countries enact cyber laws and consider the recommendations on how ECA can assist in their adoption of appropriate legal and regulatory frameworks for the knowledge economy.

II. Overview of the Current Status of Cyber Legislation in Africa

7. Cyber law has been defined as "the law which describes the legal issues related to use of inter-networked information technology (the intersection of technology and law). It is less a distinct field of law in the way that property or contract law is, as it is a domain covering many areas of law and regulation. Cyber law is the law governing computers and the Internet"[3].

8. Trading electronically differs from traditional commerce in that traditional trading was developed in a paper-based society, while e-commerce takes place in an anonymous, borderless Internet world. All the rules that were developed for trading in a real environment are inappropriate for this virtual environment. Cyber law encompasses issues such as use of electronic and digital signatures, computer crime, intellectual property, data protection and privacy, electronic authentication, liability and dispute resolution.

9. A general overview of the current status of cyber legislation in Africa shows that although an increasing number of African countries have embarked on designing and formulating information and communication (ICT) policies, the majority are still in the early stage of cyber legislation development and enactment. Of the over fifty countries in Africa, only about five countries have moved ahead of other African countries and have enacted cyber legislation to guide the area of electronic activities.

10. North Africa

- **Tunisia** was ranked top of African countries on deployment of ICT in its economy and in development of an enabling environment and infrastructure. It enacted the Electronic Commerce Law in 2000, covering the areas of application of e-commerce, tax filing, e-banking, etc. Tunisia has made remarkable progress in e-payment. It developed an e-payment system called e-Dinar, which allows Internet sales and purchases and an Internet banking system called CCPNet, which allows e-banking activations.

[3] en.wikipedia.org/wiki/Cyber_law

- **Egypt** passed Law No. 15/2004 on E-Signature and established the Information Technology Industry Development Authority (ITIDA). The law permits electronic signatures and facilitates government and business use of electronic documents. In 2006, consultations began for development of the cyber crime law.

- **Morocco** established an Interministerial Committee for Development and Promotion of Electronic Commerce.

11. Southern Africa

- In **South Africa,** the discussion paper on Electronic Commerce of July 1999 served as a starting point for the eventual promulgation of the Electronic Communication and Transactions Act No. 25/2002. The overall objective of the act is to enable and facilitate e-transactions by providing for its enforceability and building public confidence in such electronic activities. The act also provides for appointment of cyber inspectors, whose duties include investigation of cryptographic activities, authentication of service providers and inspection of websites.

- **Mauritius** has enacted the Electronic Transaction Act 2000 and Regulations – the Information Technology (Miscellaneous Provisions) Act of 1998. These provide the legal framework for validation of electronic transactions and for appointment of the Controller of Certification Authorities. They also facilitate the use of digital signatures and provide legal recognition and regulation of electronic records.

12. Although only five countries have cyber-specific laws, most African countries have outlined the need to develop cyber legislation, in their NICI e-strategy plans and objectives. Included in this category are countries such as Burundi, Cameroon, Chad, Democratic Republic of the Congo, the Gambia, Liberia, Malawi, the Niger, Nigeria, Mozambique and Swaziland. Other African countries have made significant progress in the preparation and drafting of legislation on e-commerce, though most of the draft bills have yet to be passed into law. These include:

- **Kenya**, which has already initiated the process for enacting cyber legislation. The Kenya Communications (Amendment) Bill, published in August of 2008, provides for regulation of telecoms, posts, broadcasting, electronic transactions and domain names. In the same month, the bill went through the first reading in Parliament.

- **Tanzania, where** the process commenced in 2006 with the submission of a proposal for the enactment of cyber laws by the Tanzania Law Reform Commission to the Ministry of Justice and Constitutional Affairs. It proposed separate bills on cyber crimes, regulation of electronic transactions and communications, privacy and data protection and the amendment of the Evidence Act (1967). The second development was the creation of a merged Tanzania Regulatory Authority (TCRA) to oversee postal and electronic communication industries on the mainland. The Commission for Human Rights and the Good Governance Act (16/2007) provides for the admissibility of

electronic evidence. However, this is not adequate and the bills proposed by the Tanzania Law Reform Commission still need to be enacted.

- **Uganda, which has** drafted electronic laws - the E-transaction Bill, the Computer Misuse Bill and The Electronic Signature Bill. These were approved by the Cabinet on 16 January 2008, and went to Parliament for debate. The bills are in conformity with the proposed East African Community (EAC) draft framework on cyber laws.

- **Ghana, where** the Government set up a national ICT Policy and Development Committee in August 2008, to spearhead the development of cyber laws. Ghana has drafted the Telecommunication Bill, the Electronic Transactions Bill and the National Information Technology Agency Bill.

13. At the REC level, concerted efforts have been made to develop harmonized legal frameworks for e-commerce. Several initiatives take place under the different RECs in Africa.

The Southern African Development Community (SADC)

14. In 2001, the SADC Committee of Ministers established the e-readiness task force to prepare a comprehensive study of the e-readiness status in SADC countries and come up with a plan of action. The results of the study indicated that only South Africa and Mauritius in Southern Africa had established legislation covering the broad range of issues associated with e-commerce. As a result, SADC and the USAID-funded dot-GOV Southern African ICT and Policy Reform Support ("SIPRS") Project collaborated to develop the SADC Model E-Commerce Law, to harmonize the legal framework for e-commerce. The draft version was tabled at the SADC Workshop on Harmonization of E-commerce Laws, held in Johannesburg, South Africa, on 24 November 2003. The model addressed core e-commerce issues such as cyber crime, intellectual property rights, and privacy concerns. The model was built on existing legislation in the region, and from the "Model Law on e-Commerce" formulated by the United Nations Commission for International Trade Law (UNCITRAL).

The Common Market for Eastern and Southern Africa (COMESA)

15. The European Union (EU) funded the RICTSP to support COMESA in developing policy frameworks and strategies geared towards ICT utilization. The formulation of the COMESA ICT Strategy emerged at the expert group meeting of February 2006 and was adopted by the Council of Ministers meeting in 2007. It was also presented to the Sixth Meeting of the Association of Regulators of Information and Communication of East and Southern Africa (ARICEA) in Cairo, Egypt in February 2008. This ICT strategy has four main components:

- Institutional framework – the COMESA Secretariat to spearhead the initiative;

- Legal and regulatory framework – enactment of e-signature, e-transaction, cyber crime Acts, etc.;

- Common ICT infrastructure, e.g. COMTEL and ESSAY cable projects; and

- Priority e-government services such as e-parliament and e-customs.

The Economic Community of West African States (ECOWAS)

16. In September 2004, a situational assessment survey was conducted that involved meetings with ICT policymakers within ECOWAS. It was found that there were no appreciable legislation on e-commerce in member States. As a result, a workshop was organized by ECA in Ouagadougou in December 2006. The workshop proposed that a legal framework for e-commerce and related activities had to be formulated and draft guidelines prepared and circulated to member States before adoption by ECOWAS. Following a workshop on 11 December 2007 in Lome, Togo, the participants from ECOWAS States adopted new guidelines on combating cyber crime in the subregion. As a result of this process, Ministers in charge of ICTs adopted a harmonized ICT legal framework, a Bill on e-Commerce in ECOWAS States and a model ICT framework. The acts aimed at modernizing the instruments for promoting e-commerce, preserving personal data and curbing cyber crime through the necessary subregional and national legislation.

The East African Community (EAC)

17. The five member States of EAC are also coordinating efforts to harmonize and pass cyber crime laws that would be effective throughout Burundi, Kenya, Rwanda, Tanzania and Uganda. A common information security policy on cyber crime formulated by East African countries will serve as a foundation for new laws.

18. In 2006, several EAC workshops were organized, focusing on the area of e-commerce. These included the two workshops held in April in Kampala, which were on cyber laws, e-justice and information security. In the same year, another workshop on the legal aspects of e-commerce was held in December in Nairobi. The workshops agreed on the need to formulate a regional task force to spearhead and develop model cyber laws covering e-signatures, e-transactions, authentications, cyber crimes and data and consumer protection. The task force also had to review existing laws and develop a regional legal framework for harmonization of cyber laws.

19. EAC subsequently employed a consultant in January 2008 to spearhead the process. The task force was constituted at the first task force meeting in Arusha, Tanzania, 28-30 January 2008. Two other task force meetings took place thereafter at Kampala, Uganda, in June 2008 and at Bujumbura, Burundi 10-11 September 2008. A draft framework was submitted to EAC in December 2008 and all member States agreed to have cyber laws in place by 2010. In June 2009, a meeting will be held by the task force to review the progress being made in developing national cyber laws, in line with the EAC cyber law framework.

The Arab Maghreb Union (AMU)

20. ECA initiated a study on e-commerce in Egypt, Morocco, Mauritania and Tunisia. The study was begun after the seminar held in Tangiers on ICT and the development of trade between AMU countries.. The results of the study and the plan for development of the platform were discussed during the North Africa Trade Forum on “Trade for Growth and Job Creation” held in Marrakech, Morocco, 19-21 February 2007. The trade forum came up with a proposal for setting up a regional platform for commerce.

III. Main Legal Issues of an Enabling Environment for Cyber Legislation.

21. Contract validation and the legality of electronic transactions include:

- Legal recognition and validity of e-communication as a means of executing legal acts. Removal of the legal differences between electronic contracts/messages and paper contracts;

- Making and validating e-contracts. The traditional contract principles of offer and acceptance in writing have to be met as electronic requirements; and

- Time and place of the dispatch of e-communication. The law has to state that the moment an e-communication enters a single information system outside the control of the originator, the dispatch of the communication occurs.

E-signature and authentication

22. Define signature and e-signature. Specify the criteria to be met if it is to be valid, state whether e-signatures can authenticate the party executing the signature and ensure integrity of the contents of the document to which the signature relates. The law should also establish the regulatory authority to govern the provision of authentication services.

Admissibility and evidential weight of e-communication

23. Evidence, whether contained in documents or held orally, must be admissible before a court can rely on it. With regards to paper-based evidence, weight is usually given to production of the original document. In e-transactions, this presents a problem as the distinction between an original and a copy becomes blurred and thus affects the weight given to the evidence. The law should state that in any proceedings, evidence of record may not be excluded solely because it is in an electronic form. Information in electronic form shall be given due evidential weight. The weight to be given will depend on the reliability of the manner in which the data were generated, stored or communicated.

Consumer protection

24. The law should ensure that the virtual market place is a safe and secure place to purchase goods and services and access electronic information. The consumer has to be protected from dangers such invasion of privacy, illegal or harmful goods, services and contents (e.g. pornographic material), unsolicited goods and information (spam), and so on. The law to deal with issues of cancellation rights, payment fraud and performance obligations.

Intellectual property rights

25. Cyber law should cover the intellectual property laws that relate to cyber space and its constituents. This includes copyright law (in relation to computer software, and computer source codes), trademark law (in relation to domain names), and patent law in relation to computer hardware and software. The law should offer copyright protection from information duplication and distribution on the Internet. The consequences and liability for copyright and trademark infringement should be clearly spelt out.

Data protection and privacy

26. The cyber laws should protect the fundamental rights of the privacy of an individual. Through everyday transactions, the government and other entities end up collecting immense amounts of data from individuals and businesses. The law should provide a clear distinction between what constitutes personal data and what is termed public data. Personal data has to be treated with the appropriate level of protection and should not find its way to the public domain without the express consent of the citizen.

Liability and dispute settlement

27. The era of Internet has led to problems of determining the applicable national legal system that regulates the e-transactions. A single Internet transaction may involve the laws of several jurisdictions. The legal issue may in that instance be resolved by the law being specific on areas where the country's cyber laws will be mandatory for application to consumer transactions irrespective of the myriad of laws which might impact on the transaction. The law should also be clear on whether there is immunity available to an Internet service provider (ISP) from civil and criminal liability for third party content to which they provide access or host.

E-jurisdiction

28. Traditionally, the courts within a particular country would have jurisdiction (power to adjudicate) over issues that arise within that particular country. The Internet has created a virtual borderless world in which cyber contracts are entered into by cyber citizens. Therefore, the traditional narrow definition of jurisdiction is no longer applicable. The cyber laws should state that if part of the transaction was performed in a particular country then that country has jurisdiction. In addition, even if no part of the transaction was performed in that country, if the effects are felt in that particular country then that country has jurisdiction.

E-taxation

29. E-commerce makes it easier for business to be conducted without creating the permanent establishment that would otherwise subject a seller to tax on income. It blurs the distinction between the sale of goods, provision of services and licensing of intangible assets, each of which is subject to some form of taxation. The developments in e-commerce have an impact on assessment of tax liability and identification of the growing number of taxable transactions that take place in cyberspace. Countries will want to tax transactions passing through their boarders even though parties to the transaction may not be based in that country. The law should be clear on what business transactions taking place over the Internet are subject to taxation and whether the tax authorities can tax companies incorporated offshore.

Cybercrime

30. Another key issue to be addressed by cyber legislation is the consideration and sanctioning of crimes committed in the cyber/electronic environment. The law needs to define certain cyber activities and concepts clearly, such as hacking, spam, etc., and specify the types of conduct to be criminalized. It should also amend the concept of seizure and search by empowering the law enforcement agencies to intercept communication legally. There should be adequate legal protection and enforceability of laws against cyber crimes.

IV. Overview of Existing Cyber Law Templates Used in and outside Africa

31. International efforts are underway to tackle the most important policy issues regarding ICT development. International organizations such as UNICTRAL have developed samples or templates of laws to assist countries in developing national legal and regulatory framework for e-commerce. These model laws are designed with particular attention to the need for uniform, balanced, equitable standards. In the field of cyber law, the following are some of the existing templates that can be used in and outside Africa.

UNICTRAL Model Law on e-Commerce (1996)

32. It is a draft law that has the essential procedures and rules for validation of contracts and data messages, interpretation of principles of contract such as the time and place of contracting and the formalities of writing and signature in so far as e-transactions are concerned. The second part of the model law deals with application of e-contracts for carriage of goods and their transport. It is expressed in a technologically neutral manner so that it can apply not only to existing but also to future technologies. This model was adopted and used in the drafting of cyber legislation in the Singapore Electronic Transactions Act 1998, the South Africa Communication Act No. 25/2002 and the Tunisia Electronic Commerce Law (2000), *inter alia*.

UNICTRAL Model Law on e-Signature (2001)

33. The model law provides for the legal recognition of e-signatures and in Article 6, it goes even further to provide for circumstances under which the legal requirements for a signature for commercial agreements could be satisfied by an e-signature. Article 8 provides that where an e-signature is used, the signatory shall exercise reasonable care to avoid unauthorized use of signature creation data. The model was the basic reference point in the drafting of Russia's, Egypt's and Japan's e-Signature Acts and the USA Electronic Signatures in Global and National Commercial Act 2000.

Commonwealth e-Transaction Act of 1999

34. This is also a substantive model law whose provisions basically state that under a law of the commonwealth a transaction will not be invalid just because it was conducted by use of e-communications. The Australian and UK Electronic Transaction Acts are closely modelled on this act and mirror its substantive provisions.

United Nations Convention on the Use of Electronic Communication in International Contracts (2005)

35. This convention applies to the use of e-communications in connection with formation of contracts between parties in different States. It establishes the minimum requirements for e-communication to achieve the same legal validity as traditional written contracts. It establishes that e-communications should not be denied legal effect due to the way the information is presented or retained. It also provides that a contract formed by the interaction of an automated message and a natural person shall not be denied validity on the basis that an automated message was used.

The Council of Europe's Convention on Cyber Crimes (2001)

36. The Convention seeks to harmonize the criminal substantive legal element of offences and connected provisions in the area of cyber crime and also to provide domestic criminal procedures and powers necessary for investigation of offences committed by means of computer systems, or evidence in electronic form. The convention focuses on the use of computers to commit:

- A range of traditional offences e.g. computer forgery, computer fraud and child pornography;
- Undesirable activities such as hindering the functionality of a computer system by deleting, deteriorating, transmitting or altering data; and
- Illegal data processing such as accessing a computer without authorization, by infringing security measures to obtain data, and interception of computer data.

37. Besides these international model laws, at regional level, a country can also adopt the:

SADC model Law on e-Commerce

38. This model law establishes the basic principle of non-discrimination between media, or media neutrality. Key provisions of the model are drafted to establish equivalence between paper documents and electronic messages. It also includes consideration of e-transactions, e- signatures, and data protection and privacy.

39. Other jurisdictions that may wish to adopt legislative measures to facilitate e-commerce may base their cyber law on models from other countries, such as:

Tunisia Electronic Exchanges and Electronic Commerce Act of 2000

1.	Electronic documents and electronic signature	Electronic documents and electronic signatures considered as valid as the traditional written documents and signatures
2.	National certification authority	Provides for the establishment and duties of a national certification agency
3.	Electronic certification services	Any person who intends to be registered to provide these services to be licensed by the agency
4.	Electronic commerce transactions	The merchant should provide full information on a transaction before a contract is concluded, as a consumer protection clause
5.	Protection of private information	The certification service provider may not process an individual's personal information without express approval.
6.	Infractions and penalties	Provides for penalties for non-compliance with the act's provisions

South Africa Electronic Transaction Act 25/2002

1.	Legal recognition of data messages	Computer-generated documents placed on same footing as traditional legal documents
2.	Automated transactions	Refer to e-transactions concluded by data messages
3.	Formation and validity of agreements	Agreements by means of data messages are concluded at time and place where acceptance of the offer made was received by the party making the offer
4.	Cryptograph providers	Deals with registration of such services

5.	Accreditation authority	The Act provides this role for the Director-General in the Department of Communication
6.	Unsolicited goods, service/communications	No agreement considered concluded if a consumer has not responded to unsolicited requests (spam)
7.	Protection of personal information	The data controller should have the consumer's express permission to collect, collate, process and store personal information
8.	Power to inspect, search and seize	The cyber inspector is granted these powers over any website of activity on any information system
9.	Warrant of arrest	A magistrate or judge may issue a warrant of arrest if there is reason to believe that a cyber crime has been committed
10.	Jurisdiction	The court has jurisdiction over acts committed in South Africa or whose effects are felt in South Africa

India Electronic Commerce Act of 1998

1.	Electronic records and signature	Provides that electronic records and signatures can be accorded the same level of legal recognition as paper records and signatures.
2.	Integrity and authentication of secure electronic records and signatures	Defines specific categories of records and signatures that are afforded greater evidential presumption due to their reliability and trustworthiness.
3.	Electronic contracting	Deals with the form in which an offer and acceptance may be expressed and legal recognition of electronic contracts.
4.	Effect of digital signatures	Addresses the legal issues related to the use of e-signatures.
5.	Acceptance of electronic filing and duties of certification authorities	This section authorizes any Department or Ministry to accept electronic filing of documents. Also empowers any government department to specify conditions and procedures for electronic filing.
6.	Criminal penalties	Provides penalties for internationally damaging a computer system, tampering with data, trespassing, etc.

Australia Electronic Transaction Act of 1999

1.	Validity of electronic transactions	Provides that a transaction is not invalid because it took place wholly or partly by means of one or more electronic communications
2.	Writing	If a person is required to give information in writing, that requirement is taken to have been met if the person gives the information by means of a data message
3.	Signature	If the signature of a person is required, that requirement is taken to have been met in relation to an electronic communication on which an electronic signature is used
4.	Production of document	If a person is required to produce a document that is in the form of paper, an article or other material, that requirement is taken to have been met if the person produces an electronic form of the document
5.	Retention	If a person is required to retain, for a particular period, a document that is in the form of paper, an article or other material, that requirement is taken to have been met if the person retains an electronic form of the document
6.	Time and place of dispatch and receipt of electronic communication	If an electronic communication enters a single information system outside the control of the originator, then, unless otherwise agreed between the originator and the addressee of the electronic communication, the dispatch of the

		electronic communication occurs when it enters that information system
7.	Attribution of electronic communications	With electronic communication, the purported originator is bound by that communication only if it was sent by the purported originator or with the authority of the purported originator.

V. Highlights of Best Practices in Africa and other Emerging and Developing Economies

40. As more and more countries in Africa and elsewhere in the world are enacting cyber legislation, lessons are being learnt on best practices for creating cyber laws that promote a knowledge economy. The following are some of the best practices identified:

- Focus on global harmonization, regional and international interoperability. The laws need to conform to international standards and international models in order to be integrated with the global legal framework. There are several templates such as the UNCITRAL e-commerce model law and the UNCITRAL e-signature law, the United Nations Convention on Electronic Contracting and the SADC model law that provide guidance in the drafting of cyber legislation. If the law is modelled on an international law, jurisdiction can always rely and be guided by judgments passed in those jurisdictions;

- Make the cyber law technology neutral. Some countries such as India spell out the choice of technology in the electronic transaction law; in their case it is public key cryptography. Asymmetric cryptography is the core of the current digital signature technology. It is the current standard but it is not clear if it will always be the best way to deal with e- transactions. As regards e-signature law, some countries have only validated technology- specific signatures, such as digital signatures. This is true of the US state of Utah, Italy and Germany. However, the best practice is to follow the route of an even larger number of countries that have enacted e-signature and electronic laws without linkage to a specific technology, such as the UNICITRAL model, and those of the UK, Australia and New Zealand. This way, the law is technologically neutral, flexible and able to adapt quickly to the fluid global environment;

- Separate Act for aspects of e-commerce. While development of e-commerce is encompassed under the broad umbrella of ICT, enactment of stand-alone e-transactions acts that are not all encompassing is consistent with international best practices. There is no need to have one act which addresses cyber crime, privacy and consumer protection, content such as hate speeches and pornography, intellectual property and all other issues that affect e-transactions. The Electronic Transaction Act should initially provide for the fundamental mechanism for electronic transactions by basically legalizing the electronic transactions. Even the United States of America has not tried to tackle all issues in one encompassing bill. Small amendment regulations passed through regularly. A survey was conducted by Afrika ICT Strategies Inc. (an e-legislation policy development initiative project, Dec 2006-March 2007) analysing the cyber legislation of Australia, Botswana, Egypt, India, Malaysia, Namibia, New Zealand, Pakistan, Singapore, South Africa, United Arab

Emirates, and Zambia. The research indicated that countries that had succeeded in utilizing e-commerce as an instrument for growth enacted stand-alone Electronic Transaction Acts;

- Establishment of regulatory bodies for provision of authentication services. The convergence of technologies has led to the formation of single ICT regulatory authorities. However, it should be noted that best practices indicate that electronic technologies still need a separate regulatory body to deal with authentication of e-signatures and data messages. For example, in India, the Controller of Certification Authorities is appointed by the Central Government, to regulate and control the operations of certification authorities. The duties of the Controller of Certification Authorities include licensing, certifying, monitoring and overseeing the activities of all certification authorities in India. The Tunisia Electronic Exchanges and Electronic Commerce Act 2000 provides for the establishment and duties of the National Certification Agency; and

- Need for specific law on cyber crimes. Though one can rely on such common law crimes as defamation, indecency (in regard to child pornography), crimen injuria, and fraud, there are limitations under these which might not allow successful prosecution of cyber offenders. Thus, there is need to enact cyber laws with cyber-specific crimes such as cyber smearing, cyber fraud, hacking, and so on. Countries that have such specific laws include India, Japan, Malaysia and Singapore. However, serious consideration should be given to whether certain cyber acts should be criminalized or should be left to civil remedies only.

VI. ECA-supported Areas for Practitioners in Designing and Formulating Legal and Regulatory Frameworks for the Knowledge Economy

41. Part of the focus of the ECA Division of Information for Sustainable Development is the development of e-commerce. Africa is indeed lagging behind in creating the legal and regulatory framework which will create knowledge economies. ECA follow-up activities to support countries in enacting cyber legislation should include:

Facilitating the holding of sustained cyber legislation public enlightenment/awareness campaigns

42. The public awareness campaigns must also target the private sector. The awareness programmes could also target institutions within the business community that focus more on the advantages of using cost-efficient communication technologies such as broadband, voice over Internet protocol, satellite communication and the implications of online transactions. Once the public is aware of the benefits of e-commerce, they can lobby the government to create the appropriate legal and regulatory framework. As alluded to before, Africa is lagging behind in this area due to lack of financial resources. There are huge costs involved in setting up and operating technology and ICT systems. Once there is public-heightened awareness among captains of industry, it will be much easier to encourage the private sector to play a leading funding role in ensuring that solid e-commerce legal and regulatory frameworks are in place.

Capacity-building of e- commerce institutions and human capital

43. In general, only a small percentage of lawyers in Africa are familiar with cyber legislation. This is also true of the judiciary, staff in Ministries and civil servants in relevant departments. It is important to introduce a sustained training programme suited to the needs of this category of professionals. This calls for a radical transformation in the education and training systems, science and technology policies and development strategies. Extensive technical and managerial capacity-building programmes are particularly important in view of the need to formulate and implement policies and standards and develop a proactively supporting legal and regulatory environment. ECA may consider funding, or getting donor agencies to fund partnerships for continuing legal education modules on e-commerce in various African universities or other ICT centres of learning. These capacity-building initiatives would guarantee the future of e-commerce in Africa.

Encouraging cyber laws development, cooperation and networking among African countries

44. It is better for African States to consider regional strategies rather than piecemeal approaches by individual countries for the transition to knowledge economies. ECA should continue encouraging and working with the RECs to coordinate efforts to harmonize and pass cyber crime laws within their subregions. ECA could also support member States in their efforts to translate international templates and regional draft cyber laws into national cyber legislation.