



**ECONOMIC COMMISSION  
FOR AFRICA**



**AFRICAN UNION  
COMMISSION**

**DRAFT AFRICAN UNION CONVENTION ON  
THE ESTABLISHMENT OF A  
LEGAL FRAMEWORK CONDUCTIVE TO CYBER SECURITY IN AFRICA**

**OR**

**DRAFT AFRICAN UNION CONVENTION ON  
THE CONFIDENCE AND SECURITY IN CYBERSPACE**

Version 01/09/2012

## Conceptual Framework

Based on a reappraisal of the legal and institutional climate in African Union regions as a starting point, the objective of this Convention is to propose the adoption at the level of the African Union, of a Convention establishing a credible framework for cybersecurity in Africa through organization of electronic transactions, protection of personal data , promotion of cyber security , e-governance and combating cybercrime.

### 1) Context

In a world characterized by the globalization of risks, crimes and threats to cyber security, Africa is faced with security gap which, as a result of poor mastery of security risks, increases the technological dependence of individuals, organizations and States on computer systems and networks that tend to control their information technologies needs and security facilities.

African States are in dire need of innovative criminal policy strategies that embody States, societal and technical responses to create a credible legal climate for cyber security.

It should however be observed that most African States neither have communication tools that integrate adequate means as required to achieve or guarantee a minimum level of security, nor have the human resources capable of conceiving and creating a credible legal framework.

The networked computer systems are accessible remotely and have become potential targets of cyber attacks which compromise the capacity to process, safeguard, communicate informational capital, intangible values and symbols, and the process of production or decision of those possessing such symbols, with implications for the security and survival of States and organizations.

Today, Africa more than elsewhere in the world, should as a matter of urgency offer individuals, organizations and States measures, procedures and tools for more effective management of technological, informational and legal risks. The stakes inherent in the effective control of technological risks are extremely high, and have to be addressed globally at the international level, by taking all Member States of the Union on board the security initiative, while respecting the fundamental rights of persons and of the States. Noteworthy efforts (national, community and international level) have been deployed in the realm of legal protection. In this regard, the ECA has initiated a comprehensive

harmonization project in cooperation with the authorities of UEMOA and ECOWAS. Other Regional Economic Communities have followed in the same path at a time when the States are increasingly enacting legislations on cyber security and ICTs in general. The ITU has similarly produced a guide on cyber security for use by developing countries.

This Convention pursues and deepens this momentum. It paves the way for a huge qualitative leap while giving content to political will.

## 2) Stakes and challenges

Cyber security raises multiple and complex stakes against which the magnitude of the challenges are to be measured.

The transnational nature of cybercrime calls for a focused attention on its multiple dimensions: scientific, technological, economic and financial, political and socio-cultural.

The interaction of these dimensions reinforces the complexity of cyber security which manifests at several levels:

- Informational security impacts on the security of the **digital and cultural heritage** of individuals, organizations and nations;
- The vulnerability in the normal functioning of institutions can compromise the **survival and sovereignty of States**;
- Addressing cyber security calls for clear-sighted **political will** to define and implement a strategy for development of digital infrastructure and services (e-services) and articulate a coherent, effective and controllable multi-disciplinary cyber security strategy.

The major challenges faced by Member States of the African Union are the need to:

- Achieve a level of **technological security** adequate enough to prevent and effectively control technological and informational risks;
- Build an information society that respects **values**, protects **rights and freedoms**, and guarantees the security of the property of persons, organizations and nations;

- Contribute to the knowledge economy, guarantee equal access to information while stimulating the creation of **authentic knowledge**;
- Create a climate of confidence and trust, that is:
  - **Predictable** in terms of prevention and resolution of disputes; and evolving because it takes into account the continued technological evolution;
  - **Organized**: covering the relevant sectors;
  - **Protective**: of consumers and intellectual property (civil and penal) of citizens, organizations and nations;
  - **Secured**: striking proper balance between legal and technological security;
  - **Integrated** into the international order: providing meaningful articulation between the national, regional and global levels.

### 3) Objective and goal

The objective of the Convention on Cyber Security is to contribute to the preservation of the institutional, human, financial, technological and informational assets and resources put in place by institutions to achieve their objectives. The Convention embodies the treatment of cybercrime and cyber security in its strict sense, but is not confined solely to these elements. It also embraces important elements of electronic transactions and the protection of personal data.

Its ultimate goals are eminently protective given that the Convention is geared to protecting:

- Institutions against **the threats and attacks** capable of endangering their survival and efficacy;
- The rights of **persons** during data gathering and processing against the threats and attacks capable of compromising such rights.

Similarly, the Convention seeks to:

- Reduce related institutional **intrusions or gaps** in the event of disaster;
- Facilitate the return to normal functioning at reasonable cost and within a reasonable timeframe;
- Establish the legal and institutional mechanisms likely to guarantee **normal exercise of human rights** in cyber space.

#### 4) Strategic Orientations

The Convention defines a legal mechanism based on the following five strategic orientations:

- It spells out the options for an African Union wide cyber security policy;
- It lays the foundations for an African Union wide cyber ethics and enunciates fundamental principles in the key areas of cyber security;
- It organizes electronic **transactions**, electronic signature and electronic publicity;
- It organizes the legal and institutional framework for protection of personal data;
- It lays the foundation for a penal cyber law and a penal procedure law for the treatment of cybercrimes.

**DRAFT AFRICAN UNION CONVENTION ON  
THE ESTABLISHMENT OF A LEGAL FRAMEWORK CONDUCTIVE TO  
CYBER SECURITY IN AFRICA**

**Or**

**DRAFT AFRICAN UNION CONVENTION ON  
THE CONFIDENCE AND SECURITY IN CYBERSPACE**

**PREAMBLE**

**The Member States of the African Union:**

**Considering that** this Convention on the Establishment of a Credible Legal Framework conducive to Cyber Security in Africa ( **or on the confidence and security in cyberspace** ) embodies the existing commitments of African Union Member States at sub-regional, regional and international levels to build the Information Society, seeks to define the objectives and broad orientations of the Information Society in Africa and to strengthen existing Information and Communications legislations of Member States and the Regional Economic Communities (RECs);

**Mindful of the need** to mobilize all public and private players (State, local communities, private sector enterprises, civil society organizations, the media, training and research institutions, etc) towards achieving cyber security;

**Guided by** the principles of the African Information Society Initiative (AISII) and the Regional Action Plan for the Knowledge Economy (RAPKE);

**Aware that** this Convention regulates a particularly evolving technological domain, and is a response to the high expectations of several players often with divergent interests and sets forth the security rules essential for establishing a credible digital space for **electronic transactions**, personal data protection and the combating of cybercrime;

**Convinced that** the major obstacles to electronic commerce development in Africa are linked to problems of security, particularly:

- The gaps affecting the regulation of legal recognition of data messages, as well as recognition of electronic signature;

- The absence of specific legal rules that protect consumers, intellectual property rights , personal data and information systems;
- The absence of appropriate teleservices and teleabour legislations;
- The application of electronic techniques to commercial and administrative acts;
- The probative elements introduced by digital techniques (time-date stamping, certification, etc);
- The rules applicable to cryptology devices and services;
- 
- The oversight of on-line publicity
- The absence of appropriate fiscal and customs legislations for electronic commerce;

**Convinced that** the afore-listed observations justify the need to establish an appropriate normative framework consistent with the African legal, cultural, economic and social climate; and that the objective of this Convention is therefore to offer the security and legal framework necessary for the emergence of knowledge economy in Africa;

**Considering that** protection of personal data and private life constitutes a major challenge to the Information Society for both public authorities and other stakeholders; and that the use of information and communication technologies naturally depends on the need to balance the protection of the privacy of citizens in their daily and professional activities with the guarantee of free circulation of information;

**Concerned by** the urgent need to establish a mechanism to address the dangers and risks deriving from the use of electronic data and individual records, with a view to respecting private lives and freedoms while enhancing the promotion and development of ICTs in Member States of the African Union;

**Considering the need that exists** for the harmonization in the area of cyber security legislation in Member State of the Africa Union, and to establish a mechanism capable of combating intrusions into private life likely to be generated by personal data gathering, processing, transmission, storage and use; that, by offering a standard institutional basis. The Convention ensures that any personal data treatment, regardless of its form, respects the basic freedoms and rights of individuals while also taking into

account the prerogatives of the States, the rights of local communities and the interests of businesses; that by taking on board internationally recognized best practices in matters of personal data protection it offers several regulatory platforms and modalities facilitating such protection;

**Aware of** the need, given the pervasive existence of cybercrime which constitutes a real threat to the security of computer networks and the development of the Information Society in Africa, to define broad orientations for cybercrime repression strategy in Member States of the African Union, taking into account their existing commitments at sub-regional, regional and international levels;

**Considering that** this Convention seeks, in terms of material penal laws, to modernize cybercrime repression instruments, by formulating a policy for adoption of new incriminations specific to ICTs, and aligning certain incriminations, sanctions and extant penal liability regime in Member States with the technological climate;

**Considering further** that, in terms of procedural penal laws, the Convention defines the framework for management of the classical procedures regarding information and telecommunication technologies and outlines the conditions for introduction of procedures specific to cybercrimes;

**Recalling** Decision Assembly/AU/11(XIV) of the 14<sup>th</sup> Ordinary Session of the Assembly of Heads of State and Government of the African Union on Information and Communication Technologies in Africa: Challenges and Prospects for Development, held in Addis Ababa, Ethiopia, on 1st & 2nd February 2010;

**Taking into account** the Oliver Tambo Declaration adopted by the Conference of African Ministers in charge of Information and Communication Technologies held in Johannesburg in November 2009;

Recalling the provisions of the Declaration of Addis Ababa on the Harmonisation of Cyber legislation in Africa, adopted by the experts' meeting on Cyber Legislations of Member States and RECs in Eastern, Southern and Northern Africa on 22<sup>nd</sup> June, 2012.

To be complemented by other declarations in this area (Abidjan , Khartoum, etc)

**HAVE AGREED AS FOLLOWS:**



**PART 1: Electronic transactions****Section 1: Definitions****Article I – 1:**

For the purpose of this Convention,

- 1) **Cryptology activity** means all such activity that seeks to produce, use, import, export or market cryptology tools;
- 2) **Encryption** means all techniques consisting in the processing of digital data in an unintelligible format using cryptology tools;
- 3) **Electronic commerce** means the act of offering, buying, providing of goods and services over electronic systems such as the Internet and other networks.
- 4) **Communication with the public by electronic means** refers to all circulation to the public or segments of the public, signs, signals, written matter, pictures, sounds or messages of any type without the features of a private correspondence, through an electronic communication procedure;
- 5) **Secret conventions** refers to unpublished codes required to implement a cryptology facility or service for the purpose of enciphering or deciphering operations;
- 6) **Electronic mail** means any message in the form of text, voice, sound or picture sent by a public communication network, and stored in a server of the network or in a terminal facility belonging to the addressee until it is retrieved;
- 7) Device for creating an electronic signature: a set of software or hardware elements allowing for the creation of an electronic signature (s).
- 8) Device for electronic signature verification: a set of software or hardware components allowing the verification of electronic signature.
- 9) Means of electronic payment refers to means by which the holder is able to make electronic payment transactions online.

- 10) **Cryptology** means the science of protecting and securing information particularly for the purpose of ensuring confidentiality, authentication, integrity and non-repudiation;
- 11) **Information** refers to any element of knowledge likely to be represented with the aid of devices and to be used, conserved, processed or communicated. Information may be expressed in written, visual, audio, digital and other forms;
- 12) **Cryptology tools** means the range of scientific and technical tools (equipment or software) which allows for enciphering and/or deciphering;
- 13) **Cryptology service** refers to any operation that seeks to implement cryptology facilities on behalf of oneself or of another;
- 14) **Cryptology services provider** means any person, be it a physical person or corporate body who provides cryptology services;
- 15) **Direct marketing** refers to the dispatch of any message that seeks to directly or indirectly promote the goods and services or the image of a person selling such goods or providing such services.
- 16) **Electronic signature** means data in electronic form which are attached to or logically associated with other electronic data and which serves as identification method.
- 17) **Double criminality (dual criminality)** is a crime punished in both the country where a suspect is being held and a country asking for the suspect to be handed over or transferred to.
- 18) **Indirect electronic communication** means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

## Section II: Electronic Commerce

### Chapter 1: Fields of application of electronic commerce

#### Article I – 2:

**Electronic commerce** means the act of offering, buying ,providing of goods and services over electronic systems such as the Internet and other networks.

The fields of electronic commerce comprise any online services or online commercial communications.

#### Article I – 3:

The Member States shall ensure that the activities defined in Article I – 2 of this Convention shall be exercised freely in the African Union space except:

- 1) Gambling, even in the form of legally authorized betting and lotteries;
- 2) Legal representation and assistance activities
- 3) Activities exercised by notaries in application of extant texts **or the equivalent in domestic legislation.**

#### Article I – 4:

Without prejudice to other information obligations defined by extant legislative and regulatory texts in African Union Member States shall ensure that any person exercising the activities set forth in Article I – 2 of this Convention shall provide to those for whom the goods and services are meant, easy, direct and uninterrupted access using a non-proprietary standards in regard to the following information:

- 1) Where a physical person is involved, the provider shall indicate his/her name and where it is a corporate body, its corporate name; its capital, its registration number in the register of companies or associations;
- 2) Full address of the place of establishment, electronic mail address and telephone number;

- 3) Where the person is subject to business registration formalities or registration in the national directory of businesses and associations, the registration number, the share capital and corporate headquarters;
- 4) Whether the person is subject to taxes; the tax identification number;
- 5) Where his/her activity is subject to a licensing regime, the name and address of the issuing authority; and the reference of the authorization;
- 6) Where the person is member of a regulated profession, the applicable professional rules, his/her professional title, the African Union member State in which he/she was granted such authorization, as well as the name of the order or professional body with which he/she is registered.

**Article I – 5:**

Any natural person or corporate body involved in the activities defined in Article I – 2 of this Convention, even in the absence of offer of contract and provided he/she/ it has posted a price for the said activities, shall clearly and unambiguously indicate such a price, especially where it includes taxes, delivery and other charges.

**Chapter II: Contractual responsibility of the electronic provider of goods and services**

**Article I – 6:**

The activity defined in Article I – 2 of this Convention shall be subject to the laws of the African Union Member States on the territory of which the person exercising such activity is physically presented, subject to the intention expressed in common by the said person and the recipient of the goods or services.

**Section III: Publicity by electronic means**

**Article I – 7:**

Without prejudice to Article I-4 any advertising action, irrespective of its form, accessible through online communication service, shall be clearly identified as such. It shall clearly identify the individual or corporate body on behalf of whom it is undertaken.

**Article I – 8:**

The conditions governing the possibility of promotional offers as well as the conditions for participating in promotional competitions or games where such offers, competitions or games are electronically disseminated, shall be clearly spelt out and easily accessible.

**Article I – 9:**

Direct marketing **through any form of indirect communication** including messages forwarded with automatic message sender, facsimile or electronic mails in whatsoever form, using the particulars of an individual who has not given prior consent to receiving the said direct marketing through the means indicated, shall be prohibited by the member states of the African Union.

**Article I – 10:**

The provisions of Article I – 9 above notwithstanding, direct marketing prospection by electronic mails shall be permissible where:

- 1) The particulars of the addressee have been obtained directly from him/her ,
- 2) The recipient has given consent to be contacted by the prospector partners
- 3) The direct prospection concerns similar products or services provided by the same individual or corporate body.

**Article I – 11:**

The transmission, for the purposes of direct marketing, of messages other than by means of indirect electronic communication without indicating valid particulars to which the addressee may usefully transmit a request for a stop to such communications without incurring charges other than those arising from the transmission of such request, shall be prohibited by the member states of the African Union.

**Article I – 12:**

Each Member State shall through extant legislative texts prohibit the concealing of identity of the person on behalf of whom an electronic communication is issued

**Section IV: Obligations in electronic form**

**Chapter 1: Electronic contracts**

**Article I – 13:**

The information requested for the purpose of concluding a contract or information available during contract execution may be transmitted by electronic means. It should be presumed that the use of electronic communications is proper unless the recipient has previously expressly stated a preference for an alternative means of communication.

**Article I – 14:**

A service provider or supplier, who offers goods and services in professional capacity by electronic means, shall make available the applicable contractual conditions directly or indirectly in a way that facilitates the conservation and reproduction of such conditions according to national legislations.

**Article 1 – 15:**

For the contract to be validly concluded, the offeree shall have had the opportunity to verify details of his/her order, especially the price thereof, prior to confirming the said order and signifying his/her acceptance.

**Article I – 16:**

The person offering his goods and services shall acknowledge receipt of the order so addressed to him/her without unjustified delay and by electronic means.

The order, the confirmation of acceptance of offer shall be deemed to have been received when the addressee takes due note and acknowledges receipt thereof.

**Article I – 17:**

Agreements concluded between business to business (B to B) may be exempted from the provisions of Articles I – 15 and I-16 of this Convention.

**Article I – 18:**

Any natural individual or corporate body exercising the activity defined in the first paragraph of Article I – 2 of this Convention shall, *ipso facto*, be accountable to his/her contracting partner for the proper execution of the obligations resulting from the contract, regardless of whether or not such obligations are to be executed by him/herself or by other service provider, without prejudice to his/her right of recourse against the latter.

However, he/she may discharge him/herself from the whole or part of his/her responsibility by providing proof that the non-execution or poor execution of the contract is attributable either to the contracting partner or to *force majeure*.

**Chapter II: Written matter in electronic form**

**Article I – 19**

Without prejudice to extant legislative provisions in a Member State, no person shall be compelled to take legal action by electronic means.

**Article I – 20**

Where a written matter is required to validate a legal act, a member State may by legislation establish the conditions for the functional equivalence of electronic communications to paper-based documents.

Where a matter written on paper has been subject to special legibility or presentation requirements, a written matter in electronic form shall be subject to the same requirements.

The requirement to transmit several copies of a written matter shall be deemed to have been met, where the said written matter can be reproduced in material form by the addressee.

### **Article I – 21**

The following acts shall be exempted from the provisions of Article I – 20 of this Convention:

- 1) Acts under the signature of a private individual, relating to family law and law of succession; and
- 2) Acts of civil or commercial nature under the signature of a private individual, relating to personal or real security in solidarity with domestic legislations, except where such acts have been established by a person for the purposes of his/her profession.

### **Article I – 22**

The delivery of a written matter in electronic form shall be effective when the addressee takes due note and acknowledges receipt thereof.

### **Article I – 23**

A written matter in electronic form shall be admissible for the purpose of invoicing, on equal terms as paper based written matter, provided the authenticity of the origin of the data therein and the integrity of the content are guaranteed.

### **Article I – 24**

An electronic written matter shall be admissible as proof on equal terms as paper based written matter and shall have the same evidentiary weight as the latter, provided the person who is source thereof can be duly identified and that it is prepared and conserved in conditions that guarantee its integrity.



## **Section V: Ensuring the security of electronic transactions**

### **Article I – 25**

For the purposes of this Convention,

“Electronic signature” means data in electronic form which are attached to or logically associated with other electronic data and which serves as identification method.

### **Article I – 26**

A supplier of goods must allow his clients to do their payments using electronic payment methods approved by the State according to the regulations in force in each state.

A supplier of goods or provider of services by electronic means who claims the performance of an obligation must prove its existence and when claims to liberate it must prove that the obligation is inexistence.

### **Article I – 27**

Where the legislative provisions of Member States have not laid down other provisions, and where there is no valid agreement between the parties, the judge shall resolve proof related conflicts by determining by all possible means the most plausible claim regardless of the message base employed.

### **Article I – 28**

A copy or any other reproduction of actions undertaken by electronic means shall have the same weight as the act itself, where the said copy has been certified as a true copy of the said act by bodies duly accredited by a State authority.

The certification shall culminate in the issuance of an authenticity certificate, where necessary.

## **Article I – 29**

An electronic signature on an electronic written support shall be admissible on the same terms as a signature in manuscript written on paper based matter.

The signature shall use such reliable identification procedure as guarantees its linkage with the act to which it relates.

Such procedure shall be presumed to be reliable until proved otherwise, where:  
The electronic signature has been created by a security signature device,  
The procedure guarantees the integrity of the act and the signature thereof has been identified.

## **Article I – 30**

An electronic signature created by a security device which the signatory is able to keep under his/her exclusive control and is appended to a digital certificate shall be admissible as signature on the same terms as a signature in manuscript.

## ***PART II: PERSONAL DATA PROTECTION***

### **Section 1: Terminology**

#### **Article II – 1: Definition**

For the purpose of this Convention:

- 1) **Code of conduct** means set of rules formulated by the processing official with a view to regulate the correct use of computer resources, networks and the electronic communication of the structure concerned, and approved by the protection authority.
- 2) **Consent of data subject** means any manifestation of express, unequivocal, free, specific and informed will by which the person concerned or his/her legal, judicial or treaty representative accepts that his/her personal data be subjected to manual or electronic processing.
- 3) **Recipient of data** means any person entitled to receive communication of such data other than the person concerned, the data processing official, the sub-contractor and persons who, for reasons of their functions, have the responsibility to process the data.

- 4) **Personal data** means any information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
- 5) **Sensitive data** means all personal data relating to religious, philosophical, political and labor union opinions and activities, as well as to sex life or race, health, social measures, legal proceedings and penal or administrative sanctions.
- 6) **Health data** means all information relating to the physical or mental state of the person concerned, including the aforementioned genetic data.
- 7) **Personal data file** means all structured package of data accessible in accordance with set criteria, regardless of whether or not such data are centralized, decentralized or distributed functionally or geographically.
- 8) **Interconnection of personal data** means any connection mechanism that harmonizes processed data designed for a set goal with other data processed for goals that are identical or otherwise, or interlinked by one or several processing official(s).
- 9) **Data subject** means any natural person that is the subject of personal data processing.
- 10) **Direct prospection** means any solicitation carried out through message dispatch, regardless of the message base or nature, especially messages of commercial, political or charitable nature, designed to promote, directly or indirectly, goods and services or the image of a person selling the goods or providing the services.
- 11) **Data processing official** means any natural person, public or private corporate body, or any other body or association which, on its own or jointly with others, takes the decision to gather and process personal data and determine the objective of the said processing.
- 12) **Sub-contractor** means any natural person or public or private corporate body, any other body or association which processes data on behalf of the data processing official.

- 13) **Third party** means any natural person, public or private corporate body, any other body or association other than the person concerned, the data processing official, the sub-contractor and persons entitled to process data under the direct authority of the data processing official or sub-contractor.
- 14) **Personal data processing** means any operation or set of operations conducted with or without the aid of automated or unautomated procedures and applicable to data, such as gathering, exploitation, registration, organization, conservation, adaptation, modification, extraction, safeguarding, copying, consultation, utilization, communication through transmission, dissemination or any other form of circulation, exposure or interconnection, as well as the interlocking, ciphering, deletion or destruction of personal data.

## **Section II: Legal framework for personal data protection**

### **Chapter 1: Objectives of this Convention with respect to personal data**

#### **Article II – 2:**

Each Member State of the African Union shall put in place a legal framework with a view to establishing a mechanism to combat breaches of private life likely to arise from the gathering, processing, transmission, storage and use of personal data.

The mechanism so established shall ensure that any data processing, in whatsoever form, respects the freedoms and fundamental rights of physical persons while recognizing the prerogatives of the State, the rights of local communities and the target for which the businesses were established.

### **Chapter II: Scope of application of the Convention**

#### **Article II – 3:**

The following actions shall be subject to this Convention:

- 1) Any gathering, processing, transmission, storage or use of personal data by a natural person or the State, local communities and public or private law corporate bodies;
- 2) Any automated or non-automated processing of data contained or expected to feature in a file, with the exception of the processing defined in Article II – 4 of this Convention;

- 3) Any processing of data undertaken in the territory of a Member State of the African Union;
- 4) Any processing of data relating to public security, defense, research, criminal prosecution or State security, subject to the exceptions defined by specific provisions of other extant laws.

**Article II – 4:**

This Convention shall not be applicable to:

- 1) Data processing undertaken by a natural person within the exclusive context of his/her personal or domestic activities, provided however that such data are not meant for systematic communication to third parties or for dissemination;
- 2) Temporary copies produced within the context of technical activities for transmission and access to a digital network with a view to automatic, intermediate and temporary lodging of data and for the sole purpose of offering other beneficiaries of the service the best possible access to the information so transmitted.

**Chapter III: Preliminary formalities for personal data processing**

**Article II - 5:**

The following actions shall be exempted from the preliminary formalities:

- 1) The processing mentioned in Article II – 4 of this Convention;
- 2) The processing undertaken with the sole objective of maintaining a register meant exclusively for private use;
- 3) The processing undertaken by an association or any non-profit making, religious, philosophical, political or labor union structure, provided the data so processed are consistent with the objective of the said association or structure that they relate only to the members of the association or structure and are not meant for communication to third parties.

**Article II – 6:**

With the exception of the cases defined in Article II – 5 above and in Article II – 8 and 9 of this Convention, personal data processing shall be subject to a declaration before a protection authority.

**Article II – 7:**

With regard to the most common categories of personal data processing which are not likely to constitute a breach of private life or individual freedoms, the protection authority may establish and publish standards with a view to simplifying or introducing exemptions from the declaration obligation.

**Article II – 8:**

The following actions shall be undertaken after authorization by the protection authority:

- 1) Processing of personal data involving genetic information and health research;
- 2) Processing of personal data involving information on offenses, convictions or security measures;
- 3) Processing of personal data for the purpose of interconnection of files as defined in Article II – 41 of this Convention; data processing involving national identity number or any other identification of similar nature;
- 4) Processing of personal data involving physiometric information;
- 5) Processing of personal data of public interest, especially for historical, statistical or scientific purposes.

**Article II – 9:**

The processing of personal data undertaken on behalf of the State, a public institution, a local community, a private law corporate body operating a public service, shall be in accordance with a legislative or regulatory act enacted after an informed advice of the protection authority.

Such data processing shall be undertaken for the purpose of:

- 1) State security, defense or public security;
- 2) Prevention, investigation, indictment or prosecution of criminal offenses or execution of penal convictions or security measures;
- 3) Population survey;
- 4) Compilation of personal data directly or indirectly portraying racial, ethnic or regional origin, parentage affiliation, political, philosophical or religious persuasions or labor union membership of persons, or data relating to health or sex life;

**Article II – 10:**

Requests for opinion, declarations and applications for authorization shall indicate:

- 1) The identity and address of the data processing official or, where he/she is not established in the territory of a Member State of the African Union, the identity and address of his/her duly mandated representative;
- 2) The object of the processing and a general description of his/her functions;
- 3) The interconnections envisaged or all other forms of harmonization with other processing activities;
- 4) The personal data processed, their origin and the category of the persons concerned by the processing;
- 5) Duration of conservation of the processed data;
- 6) The service or services with responsibility to undertake the processing as well as the category of persons who, for reasons of their functions or the needs of the service, have direct access to registered data;
- 7) The persons entitled to receive data communication;
- 8) The function of the person or the service before which the right of access is to be exercised;
- 9) Measures taken to ensure the security of processing actions and of data;

10) Indication regarding use of a sub-contractor;

11) Envisaged transfer of personal data to a third country that is not a Member of the African Union, subject to reciprocity.

**Article II – 11:**

The national protecting authority shall take the requisite decision within a set timeframe counting from the date of receipt of the request for opinion or authorization. Such timeframe may however be extended or not extended on the basis of an informed decision of the protection authority.

**Article II – 12:**

The opinion, the declaration or request for authorization may be addressed to the protection national authority by electronic means or by post.

**Article II – 13:**

The protection national authority may be approached by any person acting on his/her own, or through a lawyer or any other duly mandated physical person or corporate body.

**Section III: Institutional framework for protection of personal data**

**Chapter 1: Status, composition or organization**

**Article II – 14:**

Each Member State of the African Union shall establish an authority with responsibility to protect personal data.

This national authority shall be an independent administrative authority with the task of ensuring that the processing of personal data is conducted in accordance with domestic legislations.



**Article II – 15:**

The national protection authority shall inform the concerned persons and the processing officials of their rights and responsibilities.

**Article II – 16:**

Without prejudice to article II – 19 each Member State shall determine the composition of the national data Protection Authority.

**Article II – 17:**

Sworn agents may be invited to participate in audit missions in accordance with extant provisions in Member States of the African Union.

**Article II – 18:**

Members of the national protection authority shall be subject to professional secrecy in accordance with the extant texts of each Member State.

Each protection authority shall formulate rules of procedure containing, *inter alia*, rules governing deliberations, processing and presentation of cases.

**Article II – 19:**

Membership of the national protection authority shall be incompatible with membership of Government, the exercise of the functions of enterprise executive and shareholding in enterprises of information and telecommunication technologies sector.

**Article II – 20:**

Without prejudice to national legislations members of a protection authority shall enjoy full immunity for views expressed in the exercise or on the occasion of the exercise of their functions.

Members of the protection authority shall not receive instructions from any authority in the exercise of their functions.

**Article II – 21:**

Member States are engaged to provide the national protection authority human, technical and financial resources necessary to accomplish their mission.

## Chapter II: Functions of the protection authority

### Article II – 22:

The national protection authority shall ensure that the processing of personal data is consistent with the provisions of this Convention in the African Union Member States.

### Article II – 23:

The national protection authority shall ensure that ICTs do not constitute a threat to public freedoms and private life of citizens. To this end, it shall:

- 1) Respond to every request for opinion regarding personal data processing;
- 2) Inform the persons concerned and the data processing official of their rights and responsibilities;
- 3) In several cases, authorize the processing of data files, especially sensitive files;
- 4) Receive the preliminary formalities for personal data processing;
- 5) Entertain claims, petitions and complaints regarding the processing of personal data and inform the authors about the outcomes thereof;
- 6) Speedily inform the judicial authority of certain types of offenses that have come to its knowledge;
- 7) Undertake the audit of all processed personal data, through its agents or through sworn agents;
- 8) Impose sanctions, both administrative and pecuniary, on any responsible of data processing.
- 9) Update the processed personal data directory and circulate to the public;
- 10) Proffer advice to the persons and bodies engaged in personal data processing or in conducting trials or experiences likely to culminate in data processing;
- 11) Authorize cross-border transfer of personal data;
- 12) Make suggestions likely to simplify and improve legislative and regulatory framework for data processing;

- 13) Establish mechanisms for cooperation with the personal data protection authorities of third countries;
- 14) Participate in international negotiations on personal data protection;
- 15) Prepare an activity report in accordance with well-defined periodicity, for submission to either the President of the Republic, President of the National Assembly, Prime Minister or Minister of Justice.

**Article II – 24:**

The national protection authority may take the following measures:

- 1) Issuance of warning to any data processing official that fails to comply with the responsibilities arising from this Convention;
- 2) A formal demand for an end to any particular breaches within a timeframe set by the authority.

**Article II – 25:**

Where the data processing official fails to comply with the formal demand addressed to him/her, the national protection authority may impose the following sanctions after adversarial proceedings:

- 1) Provisional withdrawal of license;
- 2) Definitive withdrawal of license;
- 3) Pecuniary fine.

**Article II – 26:**

In case of emergency, where the processing or use of personal data results in violation of fundamental rights and freedoms, the national protection authority may, after adversarial proceedings, decide as follows:

- 1) Interruption of data processing;
- 2) Locking up some of the personal data processed;

- 3) Temporary or definitive prohibition of any processing at variance with the provisions of this Convention.

**Article II – 27:**

The sanctions imposed and decisions taken by the national protection authority are subject to appeal.

**Section IV: Obligations relating to the conditions governing the processing of personal data**

**Chapter 1: Basic principles governing the processing of personal data**

**Principle 1: Principle of consent and of legitimacy of personal data processing**

**Article II – 28:**

Processing of personal data shall be deemed to be legitimate where the person concerned has given his/her consent.

This requirement may however be excepted where the processing is required to:

- 1) Obtain compliance with a legal obligation to which the processing official is subject;
- 2) Execute a mission of public interest or deriving from the exercise of public authority vested in the processing official or a third party to whom the data have been communicated;
- 3) Execute a contract to which the concerned person is party or pre-contractual measures undertaken at his/her request;
- 4) Safeguard the interest or fundamental rights and freedoms of the person concerned.

## **Principle II: Principle of licitness and honesty of personal data processing**

### **Article II – 29:**

The gathering, registration, processing, storage and transmission of personal data shall be undertaken licitly, with honesty and non-fraudulently.

## **Principle III: Principle of objective, relevance and conservation of processed personal data**

### **Article II – 30:**

- 1) Data gathering shall be undertaken for a set objective that is explicit and legitimate, and the data so gathered may not be processed thereafter in a manner incompatible with the said objectives.
- 2) Data gathered shall be adequate, relevant and non-excessive in relation to the ultimate objective for which they have been gathered and subsequently processed.
- 3) The data shall be conserved for a duration not exceeding the period required to achieve the ultimate objective for which the said data have been gathered or processed.
- 4) Beyond the said period, the data may be conserved only to specifically meet the needs of data processing undertaken for historical, statistical or research purposes under the law.

## **Principle IV: Principle of accuracy of personal data**

### **Article II – 31:**

Data gathered shall be accurate and, where necessary, updated. Every reasonable measure shall be taken to ensure that incorrect and incomplete data in relation to the objective for which they were gathered and subsequently processed are deleted or corrected.

## **Principle V: Principle of transparency of personal data**

### **Article II – 32:**

The principle of transparency implies the obligation on the part of the processing official to provide information on personal data.

## **Principle VI: Principle of confidentiality and security of personal data processing**

### **Article II – 33:**

Personal data shall be processed confidentially and protected, especially where the processing involves transmission of the data in a network.

### **Article II – 34:**

Where processing is undertaken on behalf of a processing official, the latter shall choose a sub-contractor with adequate guarantees. It is incumbent on the processing official and the sub-contractor to ensure compliance with the security measures defined in this Convention.

## **Chapter II: Specific principles governing the processing of sensitive data**

### **Article II – 35:**

Members of the African Union States shall undertake necessary measures to prevent any data gathering and processing based on racial, ethnic and regional considerations, parentage relationship, political views, religious or philosophical persuasion, trade union membership, sex life and genetic information or, more generally, data on the state health of the person concerned, is prohibited in the African Union.

### **Article II – 36:**

The prohibitions set forth in Article II - 35 - shall not apply to the following types of data processing, where:

- 1) The personal data processing involves data manifestly published by the person concerned;
- 2) The person concerned has given his/her written consent, by whatsoever means, to the processing and in conformity with extant texts;

- 3) The personal data processing is required to safeguard the vital interest of the person concerned or of another person in the event that the person concerned finds him/herself in a situation whereby he/she is physically or legally unable to give such consent;
- 4) The processing of genetic data in particular is required for investigation purposes, and the exercise or defense of the right to justice;
- 5) A judicial procedure or criminal investigation has been opened;
- 6) The personal data processing is necessary in the public interest, especially for historical, statistical or scientific purposes;
- 7) The processing is required to execute a contract to which the person concerned is party or pre-contractual measures undertaken at the request of the person concerned during the pre-contractual period;
- 8) The processing is necessary to obtain compliance with a legal or regulatory obligation to which the processing official is subject;
- 9) The processing is required to execute a mission of public interest or a mission undertaken by a public authority or assigned by a public authority to the processing official or to a third party, to whom the data have been communicated;
- 10) The processing is undertaken within the framework of the legitimate activities of a foundation, association or any other non-profit making body or for political, philosophical, religious, self-help or trade union related purposes. The processing shall however concern only members of the said body or persons in regular contact with the latter in pursuance of its objective, provided the data are not transmitted to third parties without the consent of the person concerned.

**Article II – 37:**

Personal data processing for journalistic purposes or for the purpose of research or artistic or literary expression shall be admissible where the processing is meant exclusively for literary and artistic expression or for professional exercise of journalistic or research activity, in accordance with the code of conduct of these professions.

**Article II - 38:**

The provisions of this Convention shall not impede the application of national legislations relating to the print media or the audio-visual sector and the provisions of the penal code which prescribe the conditions for the exercise of the right of response, and prevent, restrict, compensate for and, where necessary, repress breaches of private life and the reputation of physical persons.

**Article II – 39:**

No decision resulting in legal consequences for a person or affect him/her to a substantial degree shall be taken, on the exclusive grounds of automated processing of personal data for the purpose of defining the profile of the person concerned or evaluating certain aspects of his/her personality.

**Article II – 40**

The data processing official shall not transfer personal data to a non-Member State of the African Union unless such a State offers sufficient level of protection of the private life, freedoms and fundamental rights of persons whose data are being or are likely to be processed.

The previous prohibition is not applicable where, before any personal data is transferred to the said third country, the data processing official shall request authorization for such transfer from the protection authority.

**Chapter III: Interconnection of personal data files****Article II – 41:**

The interconnection of files prescribed in Article II – 8 of this Convention should help attain the legal or statutory objectives that present legitimate interest for data treatment officials. It shall not result in discrimination or in erosion of the rights, freedoms and guarantees in respect of the persons concerned and nor loaded with security measures. The interconnection shall take into account on the other hand the principle of relevance of the data that are to be interconnected.



## **Section V: The rights of the person whose personal data are to be processed**

### **Chapter 1: Right to information**

#### **Article II – 42:**

The data processing official shall furnish the person whose data are to be processed with the following information, not later than the time of gathering the said data regardless of the means and facilities utilized:

- 1) His/her identity and, where necessary, that of his/her representative;
- 2) Ultimate purpose for which the data processed will be used;
- 3) Categories of data involved;
- 4) Recipient(s) to which the data are likely to be transmitted;
- 5) The capacity to request to feature no longer in the file;
- 6) Existence of the right of access to the data concerning the person and the right to correct such data;
- 7) Duration of conservation of the data;
- 8) Possibility of transfer of the data to third countries.

### **Chapter II: Right of access**

#### **Article II – 43:**

Any natural person whose personal data are to be processed may request the official conducting such processing to provide:

- 1) Such information as would enable him/her to evaluate and contest the processing;

- 2) Confirmation as to whether the personal data concerning the person are to be processed or not;
- 3) Communication of the personal data concerning the person as well as other available information on the origin of such data;
- 4) Information regarding the purpose of the processing, the categories of the personal data processed, the recipients of the processed data or the categories of the destinations to which the data are to be transmitted.

### **Chapter III: Right of opposition**

#### **Article II – 44:**

Any natural person shall have the right to object, on legitimate grounds, to the processing of the personal data concerning him/her.

He/she shall have the right to be informed before the data concerning him/her are transmitted, in the first instance, to a third party or used on behalf of the third party for the purpose of prospection; and to be expressly offered the right to object to such communication or use, free of any cost.

### **Chapter IV: Right of correction or suppression**

#### **Article II – 45:**

Any natural person may require the data processing official to rectify, complete, update, interlock or suppress, as the case may be, the personal data concerning him/her where such data are incorrect, incomplete, equivocal or outdated, or the gathering, use, communication or conservation thereof have been prohibited.

### **Section VI: Obligations of the personal data processing official**

#### **Chapter 1: Confidentiality obligations**

#### **Article II – 46:**

Processing of personal data shall be confidential. Such processing shall be undertaken exclusively by persons operating under the authority of a data processing official and exclusively on the latter's instruction.

## **Chapter 2: Security obligations**

### **Article II – 47:**

The processing official shall take all such precautions as are necessary depending on the nature of the data, and in particular, prevent such data from being distorted or damaged or from being accessed by unauthorized third parties.

## **Chapter 3: Conservation obligations**

### **Article II – 48:**

Personal data shall be conserved for a duration not exceeding the period required to achieve the ultimate objective for which the said data has been gathered or processed

## **Chapter 4: Sustainability obligations**

### **Article II – 49:**

The processing official shall take all appropriate measures to ensure that processed personal data can be utilized regardless of the technical device employed in the process.

The processing official shall, in particular, ensure that technological changes do not constitute an obstacle to the said utilization.

## ***PART III – PROMOTING CYBERSECURITY AND COMBATING CYBERCRIME***

### **Section 1: Terminology**

#### **Article III – 1:**

For the purpose of this Convention:

- 1) Electronic communication** means any transmission of signs, signals, written material, pictures, sounds or messages of whatsoever nature; to the public or a section of the public by electronic or magnetic means of communication.

- 2) **Computerized data** means any representation of facts, information or concepts in a form suitable for processing in a computer system.
- 3) **Racism and xenophobia in information and telecommunication technologies** means any written material, picture or any other representation of ideas or theories which advocates or encourages or incites hatred, discrimination or violence against any person or group of persons for reasons based on race, color, ancestry, national or ethnic origin or religion.
- 4) **Minor** means every human being below the age of eighteen (18) years in terms of the United Nations Convention on the Rights of the Child.
- 5) **Child pornography** means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where— **(A)**the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; **(B)**such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or **(C)**such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.
- 6) **Computer system** an electronic, magnetic, optical, electrochemical, or other high speed data processing device or a group of interconnected or related devices performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or devices.
- 7) **Exceeds authorized access** means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter.
- 8) **Damage** means any impairment to the integrity or availability of data, a program, a system, or information

## **Chapter 1: National cyber security framework**

### **Article III - 2: National policy**

Each Member State, shall put in place a national cyber security policy which recognizes the importance of essential information infrastructure for the nation, identifies the risks facing the nation in using the all-risk approach and broadly outlines the way by which the objectives of such policy are to be implemented.

### **Article III - 3: National strategy**

Member States shall undertake necessary strategies as they deem appropriate and adequate to implement the national cyber security policy, particularly in the area of **legislative** reform and development, awareness-raising and capacity-building, public-private partnership, international cooperation, etc. Such strategies shall define organizational structures, set objectives and timeframes for successful implementation of the cyber security policy and lay the foundation for effective management of cyber security incidents and of international cooperation.

## **Chapter 2: Legislative measures**

### **Article III – 4 : Legislations against cybercrime**

Each Member State shall adopt such legislative measures as it deems effective to adopt material criminal offenses as acts which affect the confidentiality, integrity, availability and survivability of information and telecommunication technologies systems and the data they hold or process and related infrastructure networks; as well as effective procedural measures for the arrest and prosecution of offenders. Member States have to undertake the approved language choice used in the international best practices.

### **Article III – 5: National Regulatory authorities**

Each Member State shall adopt such legislative measures as it deems necessary to confer specific responsibility on institutions, either newly established or pre-existing, as well as on the designated officials of the said institutions, with a view to conferring on them a statutory authority and legal capacity to act in all aspects of cyber security application, including but not limited to response to cyber security incidence and

**assistance / cooperation** in the field of restorative justice, forensic investigations, prosecution, etc.

### **Article III – 6 : Rights of citizens**

In adopting legislative measures in the realm of cyber security and establishing the framework for implementation thereof, each Member State shall ensure that the measures so adopted will not compromise the rights of citizens guaranteed by their national constitution, internal laws and protected by international conventions, especially the African Charter on Human and Peoples' Rights, and other rights such as freedom of expression, respect for **privacy and** the right to equitable education.

### **Article III – 7: Protection of critical information infrastructure**

Each Member State shall adopt such legislative measures as they deem necessary to identify the sectors regarded as sensitive for their national security and the health of the economy, as well as the information and telecommunication technologies systems designed to ensure the functioning of these structures as constituting **critical** information infrastructure; and, in this regard, introduce more severe sanctions for criminal activities against ICT systems in the sectors concerned and measures to improve vigilance, security and management.

## **Chapter III: National cyber security system**

### **Article III – 8: Culture of Cyber security**

- 1) Each Member State engage have to undertake measures to make it a point to inculcate a culture of cyber security in all stakeholders, namely: Governments, enterprises and the civil society, which develop, possess, manage, operationalize and use information systems and networks. The culture of cyber security shall place premium on security in information systems and networks development and on the adoption of new ways of thinking and behaving during the use of information systems as well as during communication or transactions across networks.
- 2) As part of the promotion of a culture of cyber security, Member States may adopt the following measures: devise a cyber security plan for the systems run by their governments; conduct research and devise security awareness-building programmes and initiatives for the systems and networks users; encourage the

development of a cyber security culture in enterprises; foster the engagement of the civil society; launch a comprehensive and detailed national awareness-raising programme for home users, small business , schools and children.

### **Article III –9 : Role of Governments**

Each Member State have to undertake measures to take the lead in the development of a cyber security culture within its borders and to this end enhance awareness-building, provide education and training and disseminate information to the public.

### **Article III – 10: Public-private partnership**

Each Member State have to undertake measures to adopt public-private partnership as a model to engage industry, civil society and the academia in the promotion and enhancement of a culture of cyber security.

### **Article III – 11 Education and training**

Each Member State have to undertake measures to develop capacity building measures with a view to offering training that covers all areas of cyber security in appropriate government institutions, and set standards for the private sector. Such training should help to promote information exchange among experts and security vendors, ICT owners, managers and users. Member States have to undertake measures to promote technical education for information and telecommunication technologies professionals in and outside government structures through certification and standardization of training; categorization of professional qualifications as well as development and needs-based distribution of educational materials.

## **Chapter IV: National cyber security monitoring structures**

### **Article III – 12 : Cyber security governance**

- 1) Each Member State have to undertake measures to adopt such measures as they deem necessary to establish an appropriate cyber security institutional and governance structure;
- 2) The measures adopted as per paragraph 1 of this Article **shall** seek to establish strong leadership and commitment in all aspects of the cyber security of

institutions and relevant professional bodies in each Member State. To this end, Member States have to take necessary measures to:

- i. Establish unambiguous responsibility in matters of cyber security at all levels of Government and clearly define roles and responsibilities;
  - ii. Make an unambiguous, public and transparent commitment to cyber security;
  - iii. Encourage the private sector and solicit its commitment and participation in government-led initiatives to promote cyber security.
- 3) Cyber security governance **shall** be established on the basis of a national framework capable of responding to perceived challenges and to all issues relating to information security at national level in the greatest possible number of cyber security domains.

#### **Article III – 13: Institutional framework**

Each Member State have to take necessary measures to adopt such measures as its deems necessary to establish appropriate institutions to combat cybercrime, conduct surveillance in response to cybercrime incidents and early warning, for coordination of national and cross-border cyber security problems and for global cooperation.

### **Chapter V: International cooperation**

#### **Article III – 14: Harmonization**

- 1) Member States have to undertake necessary measures to ensure that the legislative measures and / or regulations adopted to fight against cybercrime enhance the possibility of regional harmonization of these measures and respect the principle of double criminality.
- 2) Member States that don't have conventions of mutual assistance in cybercrime have to take necessary measures to encourage the signature of conventions on mutual legal assistance in accordance with the principle of double criminality while promoting the exchange of information as well as the efficient sharing of data between the organisations of Member states on a bilateral and multilateral basis.



- 3) Member States have to undertake necessary measures to encourage the establishment of institutions that exchange information on cyber threats and the evaluation of vulnerabilities such as Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIRTs).
- 4) Member States have to undertake necessary measures to make use of existing means for international cooperation to respond to cyber threats, improve cybersecurity and stimulate dialogue among stakeholders. These means may be international, intergovernmental or regional or based on private-public partnerships.

## **Section II: Material penal law**

### **Chapter 1: Offenses specific to Information and Communication Technologies**

#### **Section 1: Attack on computer systems**

##### **Article III – 15**

Each Member State of the African Union have to take necessary legislative measures to set up as a penal offense the fact of accessing or attempting to access fraudulently a part or the whole of a computer system or exceeding an authorized access.

##### **Article III – 16**

Each Member State of the African Union have to take necessary legislative or regulatory measures to set up as penal offense the fact of accessing or attempting to access fraudulently a part or the whole of a computer system or exceeding an authorized access with the intent to commit another offense or facilitate the commission of such an offense.

##### **Article III – 17**

Each Member State of the African Unions have to take necessary legislative or regulatory measures to set up as a penal offense the fact of retaining oneself or attempting to retain oneself fraudulently in a part or the whole of a computer system.

**Article III – 18**

Each Member State of the African Union have to take necessary legislative or regulatory measures to set up as a penal offense the fact of hampering, distorting or attempting to hamper or distort the functioning of a computer system.

**Article III – 19**

Each Member State of the African Union have to take necessary legislative or regulatory measures to set up as a penal offense the fact of introducing or attempting to introduce data fraudulently in a computer system.

**Article III – 20**

Each Member State of the African Union have to take necessary legislative or regulatory measures to set up as a penal offense the fact of damaging or attempting to damage, delete or attempting to delete, spoil or attempting to spoil, alter or attempting to alter, modify or attempting to modify fraudulently computer data.

**Article III – 21**

The Member States have to take necessary legislative or regulatory measures to compel ICT product vendors to submit their products for vulnerability and guarantee tests to be conducted by independent experts and researchers and to divulge to the public any form of vulnerability found in the said products and the measures recommended for a solution thereto.

**Article III –22**

Each Member State of the African Union have to take necessary legislative or regulatory measures to set up as a penal offense the fact of illegally producing, selling, importing, possessing, disseminating, offering, ceding or circulating a computer equipment, a programme, or any device or data designed or specially adapted to commit an offense, or illegally generate or produce a password, or an access code or similar computerized data allowing access to the whole or part of a computer system.

**Section II: Attack on computerized data****Article III – 23**

Each Member State of the African Union have to take necessary legislative or regulatory measures to set up as a penal offense the fact of intercepting or attempting to intercept fraudulently computerized data by technical means, or in excess of authorization or to impair the confidentiality of information during non-public transmission of the said data to, from or within a computer system.

**Article III – 24**

Each Member State of the African Union have to take necessary legislative or regulatory measures to set up as a penal offense the fact of producing or manufacturing a range of digital data by fraudulently introducing, deleting or suppressing computerized data held, processed or transmitted by a computer system, resulting in fake data, with the intention that the said data would be taken into account or used for illegal purposes as if they were the original data.

**Article III – 25**

Each Member State of the African Union have to take necessary legislative or regulatory measures to set up as a penal offense the fact of using data obtained fraudulently from a computer system with a full knowledge of the case.

**Article III – 26**

Each Member State of the African Union have to take necessary legislative or regulatory measures to set up as a penal offense the fact of obtaining fraudulently, for oneself or for another person any advantage whatsoever by introducing, altering, deleting or suppressing computerized data or any other form of attack on the functioning of a computer system.

**Article III –27**

Each Member State of the African Union have to take necessary legislative or regulatory measures to set up as a penal offense the fact, even out of negligence, of processing or causing the processing of personal data without having respected the preliminary formalities for the processing.

**Article III – 28**

Each Member State of the African Union have to take necessary legislative or regulatory measures to set up as a penal offense the fact of participating in an association formed or in an understanding established with a view to preparing or committing one or several of the offense (s) defined in this Convention.

**Section III: Content related offenses****Article III – 29**

Each Member State of the African Union have to take necessary legislative or regulatory measures to set up as a penal offense the fact of producing, registering, offering, **making**, circulating, disseminating and transmitting a picture, a representation of child pornography or any child pornography material by means of a computer system.

**Article III – 30**

Each Member State of the African Union have to take necessary legislative or regulatory measures to set up as a penal offense the fact of procuring for oneself or for another person, importing or causing to be imported and exporting or causing to be exported a picture or representation of child pornography by means of a computer system.

**Article III – 31**

Each Member State of the African Union have to take necessary legislative or regulatory measures to set up as a penal offense the fact of possessing a picture or a representation of child pornography in a computer system or in whatsoever means for holding computerized data.

**Article III – 32**

Each Member State of the African Union have to take necessary legislative or regulatory measures to set up as a penal offense the fact of facilitating access to pictures, documents, sounds or any other child pornography material or representation of pornography of a minor.

**Article III – 33**

Each Member State of the African Union have to take necessary legislative or regulatory measures to set up as a penal offense the offenses defined in this Convention where they have been committed in an organized group, and liable to the maximum punishment prescribed for such offense.

**Article III – 34**

Each Member State of the African Union have to take necessary legislative or regulatory measures to set up as a penal offense the fact of creating, downloading, disseminating or circulating in whatsoever form, written matters, messages, photographs, drawings or any other presentation of ideas or theories of racist or xenophobic nature using an a computer system.

**Article III – 35**

Each Member State of the African Union have to take necessary legislative or regulatory measures to set up as a penal offense an attack perpetrated through a computer system, with the intention of committing a criminal offense against any person for reasons of his/her membership of a group characterized by race, color, ancestry, national or ethnic origin or religion where such membership serves as a pretext for any of these offenses, or a against a group of persons distinguishable by any of these characteristics.

**Article III – 36**

Each Member State of the African Union have to take necessary legislative or regulatory measures to set up as a penal offense an abuse committed by means of a computer system against any person for reasons of his/her membership of a group characterized by race, color, ancestry, national or ethnic origin or religion where such membership serves as a pretext for any of these offenses, or against a group of persons distinguishable by any of these characteristics.

**Article III – 37**

Each Member State of the African Union have to take necessary legislative or regulatory measures to set up as a penal offense the deliberate fact of denying,

approving or justifying acts of genocide or crimes against humanity by means of a computer system.

### **Article III – 38**

Each Member State of the African Union have to take necessary legislative or regulatory measures to ensure that, in case of conviction, the national tribunals will give a ruling for confiscation of the materials, equipment, tools, computer programmes and all other devices or data belonging to the convicted person and used to commit any of the offenses mentioned in this Convention.

### **Section III: Offenses relating to electronic message security measures**

#### **Article III – 39**

Each Member State of the African Union have to take necessary legislative or regulatory measures to ensure that the evidence in respect of criminal offences is admissible to establish offenses under national criminal laws, provided such evidence has been presented during debate and discussed before the judge, that the person from which the evidence emanates can be duly identified and the said evidence has been prepared and conserved under conditions likely to guarantee its integrity.

### **Chapter II: Adapting certain information and communication technologies offenses**

#### **Section 1: Violation of property**

##### **Article III - 40**

Each Member State of the African Union have to take necessary legislative or regulatory measures to set up as an aggravating circumstance the use of information and telecommunication technologies to commit offenses such as theft, fraud, possession of stolen goods, abuse of trust, extortion of money, terrorism, money laundering, etc.

**Article III – 41**

Each Member State of the African Union have to take necessary legislative or regulatory measures to set up as a legal offense the violation of property such as theft, fraud, possession of stolen goods, abuse of trust, extortion of money and blackmail involving computer data.

**Article III – 42**

Each Member State of the African Union have to take necessary legislative or regulatory measures to expressly include “means of digital electronic communication” such as the internet in the enumeration of the public dissemination facilities defined in the penal texts of Member States.

**Article III – 43**

Each Member State of the African Union have to take necessary criminal legislative measures required to restrict access to protected systems which have been designated to be critical national defense infrastructure because they store computerized files containing critical national security information.

**Section II: Criminal liability for corporate persons****Article III –44**

Each Member State of the African Union have to take necessary legislative measures to ensure that corporate bodies other than the State, local communities and public institutions can be held responsible for the offenses defined in this Convention, committed on their behalf by their organs or representatives. The liability of the said corporate bodies does not exclude that of the physical persons who are the authors or accomplices of the same offenses.

## **Chapter III: Adapting certain sanctions to the Information and Communication Technologies**

### **Section 1: Penal sanctions**

#### **Article III – 45**

Each Member State of the African Union have to take necessary legislative measures to ensure that the offenses defined in this Convention attract effective, proportional and deterrent penal sanctions.

#### **Article III – 46**

Each Member State of the African Union have to take necessary legislative measures to ensure that the offenses defined in this Convention attract appropriate punishments according to domestic legislations.

#### **Article III – 47**

Each Member State of the African Union have to take necessary legislative measures to ensure a corporate body declared liable in terms of this Convention is subject to effective, proportional and deterrent sanctions which include penal fines.

### **Section II: Other penal sanctions**

#### **Article III – 48**

Each Member State of the African Union have to take necessary legislative measures to ensure that, in the case of conviction for an offense committed by means of digital communication facility, the competent jurisdiction or the judge handling the case gives a ruling imposing additional punishment.

#### **Article III – 49**

Each Member State of the African Union have to take necessary legislative measures to ensure that, in the case of conviction for an offense committed by means of information and telecommunication technology the competent judge can make a further binding ruling for the dissemination of the decision by extract and via the same facility at the



expense of the convicted person, in accordance with the modalities prescribed in domestic laws.

### **Section III: Procedural law**

#### **Article III – 50**

Each Member State of the African Union have to take necessary legislative measures to ensure that where the data held in a computer system or in a facility that allows for the conservation of computerized data in the territory of a Member State, are useful in revealing the truth, the investigating judge will issue a search or seizure warrant , to access or seize a computer system or part of the system or any other computer systems where the said data are accessible from the original system or available in the initial system.

#### **Article III – 51**

Each Member State of the African Union have to take necessary legislative measures to ensure that where an investigating judge discovers that the data held in a computer system are useful for revelation of the truth, but that seizure of the facility does not seem appropriate, the said data as well as all such data as are required to unravel the case, shall be copied into a computer storage facility that can be seized and sealed off, in accordance with the modalities defined in the legislations of Member States.

#### **Article III – 52**

Each Member State of the African Union have to take necessary legislative measures to ensure that criminal intelligence officers can, for the purposes of investigation or execution of a judicial delegation, undertake the operations set forth by this Convention.

### **Section IV: Offenses specific to Information and Communication Technologies**

#### **Article III –53**

Each Member State of the African Union have to take necessary legislative measures to ensure that, where the imperatives of the information so dictate, particularly where there are reasons to believe that the information stored in a computer system are particularly susceptible to loss or modification, the investing judge may issue a warrant to any person to conserve and protect the integrity of the data in his/her possession or

under his/her control, for a duration of not more than two years in the interest of the proper conduct of the judicial investigation. The custodian of the said data or any other person with responsibility to conserve the data shall be expected to keep the secrets contained in the data.

#### **Article III – 54**

Each Member State of the African Union have to take necessary legislative measures to ensure that the violation of the secrets stored in a computer system attracts same punishments applicable to the offense of violation of professional secrets.

#### **Article III – 55**

Each Member State of the African Union have to take necessary legislative measures to ensure that, where the imperatives of the information so dictate, the investigating judge can use appropriate technical means to gather or register in real time the data in respect of the content of specific communications in its territory, transmitted by means of a computer system or compel a service supplier to gather and register the data within the framework of his/her technical capacities, using the existing technical facilities in its territory or that of States parties, or provide support and assistance to the competent authorities towards the gathering or registration of the said computerized data.

### ***PART IV: COMMON AND FINAL PROVISIONS***

#### **Section 1: Monitoring mechanism**

#### **Article IV – 1**

Member States of the African Union delegate the President of the Commission to conduct a study and implement a monitoring operational mechanism for this Convention.

This mechanism is to:

- a) Promote and encourage the adoption and application in the African continent of cyber security building measures in electronic systems and the ways to combat cybercrime and breaches of the rights of individuals in cyberspace;
- b) Assemble documents and information on cyber security needs as well as on the nature and extent of cybercrime and breaches of the rights of individuals in cyberspace;
- c) Devise methods to analyze cyber security needs as well as on the nature and extent of cybercrime and breaches of the rights of individuals in cyberspace; disseminate information and sensitize public opinion on the negative effects of these phenomena;
- d) Advise African governments on the best way to promote cyber security and combat the scourge of cybercrime and breaches of the rights of individuals in cyberspace;
- e) Gather information and undertake analysis on the misuse of information networks and computer systems operating in Africa and transmit such information to competent national authorities;
- f) Formulate and promote the adoption of harmonized codes of conduct for the use by cyber security public agents;
- g) Establish partnerships with the African Commission and the African Court on Human and Peoples' Rights, the African civil societies, governmental, inter-governmental and non-government organizations with a view to facilitating dialogue on combating cybercrime and breaches of the rights of individuals in cyber space;
- h) Submit regular reports to the Executive Council of the African Union on the progress made by each State Party in the implementation of the provisions of this Convention;
- i) Discharge such other tasks relating to cybercrime and breaches of the rights of individuals in cyberspace as may be assigned to it by the policy organs of the African Union.

## **SECTION 2: FINAL PROVISIONS**

### **Article IV – 2: Signature, ratification, accession and entry into force**

- 1) This Convention shall be open to signature, ratification or accession by Member States of the African Union.
- 2) It shall enter into force thirty (30) days after the deposit of the fifteenth instrument of ratification or accession.
- 3) For each State Party that ratifies or accedes to this Convention after the date of the deposit of the fifteenth instrument of ratification, the Convention shall enter into force thirty (30) days after the date of the deposit of the instrument of ratification or accession by that State Party.

### **Article IV – 3: Reservations**

- 1) Any State Party may, at the moment of adoption, signature, ratification or accession of this Convention file reservations in respect to its provisions provided each reservation concerns one or several specific provisions and is not incompatible with the objectives and purposes of this Convention.
- 2) Any State Party that has filed a reservation may withdraw such reservation as soon as circumstance so permit. The withdrawal will enter into force by a notification addressed to the Chairperson of the Commission.

### **Article IV – 4: Amendment**

- 1) Amendments to this Convention may be proposed by any State Party and have to be communicated by a written request to the Chairperson of the Commission.
- 2) The Chairperson of the Commission shall transmit the amendment request to all the States Parties which shall examine the said request only six months after the date of its transmission.
- 3) The amendment shall enter into force after its approval by two-thirds majority of Member States of the African Union.

**Article IV – 5: Denunciation**

Any State Party may denounce this Convention by written notification addressed to the Chairperson of the Commission. The said denunciation shall take effect six (6) months after the date of receipt of the notification by the Chairperson of the Commission.

**Article IV – 6: Depository**

- 1) The Chairperson of the Commission shall be the depository of this Convention and the amendments thereto.
- 2) The Chairperson of the Commission shall update all the States Parties on the status of signature, ratification and accession as well as the entry into force, amendment requests introduced by the States, approval of amendment proposals and denunciations.
- 3) Upon the entry into force of this Convention, the Chairperson of the Commission shall register same with the Secretary General of the United Nations in accordance with Article 102 of the United Nations Charter.

**Article IV – 7: Authentic texts**

This Convention, is drawn up in four (4) original texts in Arabic, English, French and Portuguese languages, all texts being equally authentic, shall be deposited with the Chairperson of the Commission. The chair person shall transmit certified copies to each Member State of the African Union.

**IN WITNESS WHEREOF, WE THE HEADS OF STATE AND GOVERNMENT OF THE AFRICAN UNION OR OUR DULY MANDATED REPRESENTATIVES, HAVE ADOPTED THIS CONVENTION.**

**Done at ..... on.....**