ECONOMIC COMMUNITY OF
WEST AFRICAN STATES

COMMUNAUTE ECONOMIQUE
DES ETATS DE L'AFRIQUE
DE L'OUEST

SIXTY-SIXTH ORDINARY SESSION OF THE COUNCIL OF MINISTERS

Abuja, 17 – 19 August 2011

DIRECTIVE C/DIR. 1/08/11 ON FIGHTING CYBER CRIME WITHIN ECOWAS

THE COUNCIL OF MINISTERS,

MINDFUL of Articles 10, 11 and 12 of the ECOWAS Treaty as amended, establishing the Council of Ministers and defining its composition and functions;

MINDFUL of Articles 27, 32 and 33 of the said Treaty on Science and Technology, and on the areas of Communication and Telecommunications;

MINDFUL of Article 57 of the said Treaty on judicial and legal cooperation, which provides that Member States undertake to promote judicial cooperation with a view to harmonizing judicial and legal systems;

MINDFUL of the ECOWAS Supplementary Act A/SA 1/01/07 of 19 January 2007 on the harmonization of the policies and regulatory framework of the Information and Communication Technology sector (ICT);

MINDFUL of the ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS;

MINDFUL of the ECOWAS Supplementary Act A/SA.2/01/10 on Electronic Transaction within ECOWAS;

MINDFUL of Convention A/P1/7/92 of ECOWAS relating to the Mutual Assistance in Criminal Matters;

MINDFUL of Convention A/P1/94 relating to extradition;

MINDFUL of the cooperation as regards matters of criminal policing between the member States of ECOWAS which provides the pooling of expertise and sharing of experiences by security services with a view to establishing an efficient method of police investigations;

CONSIDERING that the use of information and communication technologies, among others, the internet or cybernetics, has generated an upsurge of reprehensible acts;

NOTING that cyber crime is a new phenomenon that requires the definition of specific offences that must be substantially linked with conventional offences such as theft, swindling, the receipt of stolen goods, blackmail, and damages caused by the use of the internet;

CONSCIOUS that criminal acts committed by means of internet require the identification of a legal regime and a suitable punishment because of the level of damage they generate;

DESIROUS to adopt a framework for criminal liability in order to effectively fight against cyber crime and provide for efficient and reliable international cooperation.

HAVING OBTAINED THE OPINION of the ECOWAS Parliament dated 23 May 2009;

PRESCRIBES:

CHAPTER I

GENERAL PROVISIONS

Article 1 Definitions

For the purposes of this Directive:

Electronic communication means making communication available to the general public or a category of the public through a process of electronic or electromagnetic means, signs, signals, written documents, images, sounds or messages of any kind;

Computer data: any representation of facts, information or concepts in a form suitable for processing in a computer system;

Racism and xenophobia in relation to ICTs refer to any document, image or any other depiction of ideas or theories, which advocates or encourages hatred, discrimination or violence against a person or group of persons by reason of their race, colour, ancestry, affiliation or their national or ethnic origin or religion, to the extent that this reason serves as a pretext for one or the other of such elements or incites such acts;

Minor: any person under the age of eighteen (18) as stipulated in the United Nations Convention on the Rights of the Child;

Child pornography: any data of whatever nature or form, that visually depicts a minor engaged in a sexually explicit conduct or realistic images representing a minor engaged in a sexually explicit conduct;

Computer system: any isolated or non-isolated device or group of interconnected devices that all or in part carries out automatic processing of data pursuant to a programme.

Information Technology and Communication (ITC): technologies used to gather, store, use and send information, including technologies that involve the use of computers or any communication system, including any telecommunication system.

Article 2 Objective

The objective of this Directive is to adapt the substantive criminal law and the criminal procedure of ECOWAS Member States to address the cybercrime phenomenon.

Article 3 Scope

This Directive shall be applicable to all cyber crime-related offences within the ECOWAS sub-region as well as to all criminal offence whose detection shall require electronic evidence.

CHAPTER II

OFFENCES SPECIFICALLY RELATED TO INFORMATION AND COMMUNICATION TECHNOLOGIES

For the purposes of this Directive, the following shall constitute offences:

Article 4 Fraudulent access to computer systems

Fraudulent access to computer systems **is** the act by which a person fraudulently accesses or attempts to access the whole or part of a computer system.

Article 5 Fraudulently remaining in a computer system

Fraudulently remaining in a computer system is the act by which a person fraudulently remains or attempts to remain within the whole or part of a computer system.

Article 6 Interfering with the operation of a computer system

Interfering with the operation of a computer system is the act by which a person impedes, alters or attempts to impede or alter the functioning of a computer system.

Article 7 Fraudulent input of data in a computer system

Fraudulent input of data in a computer system is the act by which a person fraudulently inputs or attempts to input data into a computer system.

Article 8 Fraudulent interception of computer data

Fraudulent interception of computer data is the act by which a person fraudulently intercepts or attempts to intercept computer data during their non-public transmission to, from or within a computer system using technological means.

Article 9 Fraudulent modification of computer data

Fraudulent modification of computer data is the act by which a person fraudulently damages or attempts to damage, delete or attempts to delete, worsen or attempting to worsen, alter or attempts to alter, modify or attempt to modify computer data.

Article 10 Computer data forgery

Computer data forgery is the act by which a person produces or manufactures a set of digital data through fraudulent input, deletion or suppression of computer data stored, processed or transmitted by a computer system, resulting in counterfeit data, with the intent that it be considered or used for legitimate purposes as if it were genuine.

Article 11 Obtaining benefit from Computer related fraud

Obtaining benefit from Computer related fraud is the act of obtaining fraudulently for oneself or for another person material or economic benefit through the input, alteration, deletion or suppression of computer data or through any other form of interference with the functioning of a computer system.

Article 12 Fraudulent manipulation of personal data

Fraudulent manipulation of personal data is the act by which a person, even through negligence, processes personal data or causes personal data to be processed without having complied with the prerequisite conditions stipulated by the relevant law on personal data provided for in each Member State.

Article 13 Use of forged data

Use of forged data is the act by which a person knowingly uses forged data.

Article 14 Obtaining equipment to commit an offence

Obtaining equipment to commit an offence is the act by which a person knowingly without any legitimate reason produces, sells, imports, possesses, distributes, offers, transfers or makes available equipment, computer programmes, or any device or data, any password, access code or similar computer data by which they

commit any offence as stipulated in this Directive.

Article 15 Participation in an association or agreement to commit computer offences

Participation in an association or agreement to commit *computer* offences is the act by which a person participates in an association that is formed or an agreement that is established for the purpose of preparing or committing one or several of the offences described in this Directive.

Article 16 Production of child pornography or pornographic representation

Production of child pornography or pornographic representation is the act by which a person produces, records, offers or makes available, distributes or transmits child pornography or pornographic representation through a computer system.

Article 17 Import or export of child pornography or pornographic representation

Import or export of child pornography or pornographic representation is the act by which a person procures for oneself or for another person, imports or causes to be imported, exports or

causes to be exported, child pornography through a computer system.

Article 18 Possession of child pornography or pornographic representation

Possession of child pornography or pornographic representation is the act by which a person possesses child pornography or pornographic representation through a computer system or through any other computer data storage medium.

Article 19 Facilitation of access of minors to pornography, documents, sound or pornographic representation

Facilitation of access of minors to pornography, documents, sound or pornographic representation is the act by which a person facilitates access of a minor to pornographic pictures, sounds or representation.

Article 20 **Possession of racist or xenophobic written documents or pictures through a computer system**

Possession of racist or xenophobic written documents or pictures through a computer system is the act by which a person creates, downloads, disseminates, or makes available in whatever form, written documents, messages, photographs, drawings or any other depictions of racist and xenophobic ideas and theories by means of a computer system.

Article 21 **Threat through a computer system**

Threat through a computer system is any threat through a computer system to commit a criminal offence against a person by reason of his affiliation to a group that is characterised by race, colour, ancestry, ascendants, religion, national or ethnic origin , to the extent that this affiliation serves as a pretext for such a threat to that person or a group of persons that is distinguished by one of the foregoing characteristics.

Article 22 **Abuse through a computer system**

Abuse through a computer system is any abuse to a person through a computer system by reason of his belonging to a group that is characterised by race, colour, ancestry, ascendants, religion, national or ethnic origin, to the extent that this affiliation serves as a pretext for such an abuse to the person or a group of persons that is distinguished by the foregoing characteristics.

Article 23 **Denying or justifying acts or crimes against humanity by means of a computer system**

Denying or justifying acts or crimes against humanity by means of a computer system is any intentional act to deny, approve or justify established acts of genocide or crimes against humanity by means of a computer system.

CHAPTER III

INCORPORATING TRADITIONAL OFFENCES INTO INFORMATION AND COMMUNICATION TECHNOLOGY OFFENCES

Article 24 Aggravating Circumstances of Common Law Offences

Under this Directive, the use of ICTs to commit common law offences such as theft, fraud, possession of stolen goods, breach of trust, extortion, terrorism, and money laundering or organised crimes shall constitute a higher degree of offence than the common law offences.

Article 25 Violations of computer data, software and programme

Under this Directive, theft, fraud, possession of stolen goods, breach of trust, extortion, acts of terrorism, and counterfeiting

relating to computer data, software and programme shall constitute an offence.

Article 26 Media offence committed through electronic means of communication

Media offences committed through electronic means of communication under this Directive shall be subjected to the provisions relating to media offences which are applicable in Member States.

Article 27 Liability of Corporate Bodies other than Public Entities

Any corporate body, excluding the State, local authorities and public establishments, shall be held liable for any of the offences described in this Directive that are committed for their benefit by their representatives. Such liability shall not exclude the liability of individuals who commit such acts or abet the commission of such acts.

CHAPTER IV

SANCTIONS

Article 28 Major penalties

1) The offences stipulated under this Directive shall be punishable under the criminal Court of Member States. Sanctions shall be proportionate and dissuasive.

2) Any corporate body found liable under this Directive shall be punishable by proportionate and dissuasive sentences, including criminal and civil penalties.

Article 29 Supplementary Penalties

1. In the event of conviction for an offence committed through an electronic communication medium, the relevant jurisdiction may decree supplementary sanctions.

2. In the event of conviction, the court may decide that materials, equipment, instruments, computer programmes or data, as well as proceeds from an offence and belonging to the convicted person be confiscated.

3. Conviction decisions shall be published in the National Gazette of Member States and in an electronic medium at the expense of the convict.

CHAPTER V:

RULES OF PROCEDURE

Article 30 Search or access to a computer system

1. The national competent authority may carry out searches or effect seizures or have access to any computer system in order to establish the truth.

2. However, where seizure of the electronic medium is undesirable, the data required to understand it shall be copied on a computer data storage medium and sealed.

Article 31 Expedited preservation of data

Where the exigencies of information so require, and where there is reason to believe that computerized data recorded in a computer system can be lost, the national competent authority shall order any individual to keep and protect in secret the integrity of data in his possession or under his control within a time line set by a Member State.

Article 32 Method of Proof

Electronic evidence shall be accepted as proof to establish an offence provided the person from whom they emanate can be identified and that they are kept in such conditions as to guarantee their integrity.

Article 33 Judicial Cooperation

1. Where Member States are informed by another Member State of the alleged commission of an offence as defined in this Directive, such Member States shall cooperate in the search for and establishment of that offence, as well as in the collection of evidence pertaining to the offence.

2. Such cooperation shall be carried out in line with relevant international instruments and mechanisms on international cooperation in criminal matters.

CHAPTER VII:

FINAL PROVISIONS

Article 34 Publication

This Directive shall be published by the Commission in the Community Official Journal within thirty (30) days of the date of signature by the

Chairman of the Council of Ministers. It shall equally be published by each Member State in its national Gazette thirty (30) days after notification by the Commission.

Article 35 Implementation

1. Member States shall adopt the necessary legislative, regulatory and administrative measures in order to comply with this Directive not later than 1st January 2014.

2. The measures referred to in Paragraph 1 of this Article should make reference to this Directive or shall be accompanied by such reference upon their official publication.

3. Member States shall inform the ECOWAS Commission of the measures they will adopt to comply with this Directive.

4. Member States shall notify the President of the Commission of the difficulties they encounter in implementing this Directive. The President of the Commission shall report such difficulties at the next session of the Council of Ministers which shall, in turn, take the appropriate measures to ensure the effective implementation of this Directive.

DONE AT ABUJA, THIS 19TH DAY OF AUGUST 2011

.....

H.E. OLUGBENGA ASHIRU

CHAIRMAN

FOR COUNCIL