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

ECONOMIC COMMUNITY OF
WEST AFRICAN STATES

SOIXANTE SIXIEME SESSION ORDINAIRE DU CONSEIL DES MINISTRES

Abuja, 17 – 19 Août 2011

DIRECTIVE C/DIR/1/08/11 PORTANT LUTTE CONTRE LA CYBERCRIMINALITE DANS L'ESPACE DE LA CEDEAO

LE CONSEIL DES MINISTRES,

VU les Articles 10, 11 et 12 du Traité de la CEDEAO tel qu'amendé, portant création du Conseil des Ministres et définissant sa composition et ses fonctions ;

VU les articles 27, 32 et 33 dudit Traité relatifs à la science et à la technologie, et aux domaines des communications et des télécommunications ;

VU l'article 57 dudit Traité relatif à la coopération judiciaire et juridique qui prescrit que les Etats membres s'engagent à promouvoir la coopération judiciaire en vue d'harmoniser les systèmes judiciaires et juridiques;

VU l'Acte additionnel A/SA 1/01/07 du 19 janvier 2007 de la CEDEAO relatif à l'harmonisation des politiques et du cadre réglementaire du secteur des Technologies de l'Information et de la Communication (TIC) ;

VU l'Acte Additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel dans l'espace CEDEAO ;

VU l'Acte Additionnel A/SA.2/01/10 relatif aux transactions électroniques dans l'espace CEDEAO ;

VU la Convention A/P1/7/92 de la CEDEAO relative à l'entraide judiciaire en matière pénale ;

VU la Convention A/P1/8/94 de la CEDEAO relative à l'Extradition ;

VU l'Accord de coopération en matière de police criminelle entre les Etats membres de la CEDEAO qui prescrit la mise en commun des compétences et partage d'expérience par les services de sécurité en vue d'accélérer de façon efficace les enquêtes policières ;

CONSIDERANT que l'utilisation des Technologies de l'Information et de la Communication entre autres l'Internet ou la cybernétique a engendré la recrudescence d'actes répréhensibles de tous ordres ;

NOTANT que la cybercriminalité est un phénomène nouveau qui nécessite la définition des infractions spécifiques, lesquelles doivent être rattachées consubstantiellement aux infractions classiques, tels que le vol, l'escroquerie, le recel, le chantage en raison de la nature du préjudice causé au moyen de l'utilisation de l'Internet ;

CONSCIENT que les actes répréhensibles commis au moyen de l'Internet nécessitent donc une qualification au plan légal et une répression appropriée en raison de la gravité des préjudices qu'ils engendrent ;

DESIREUX d'adopter un cadre de répression pénale en vue de lutter efficacement contre la cybercriminalité, ainsi que de permettre une coopération diligente et viable à l'échelle internationale;

APRES AVIS du Parlement de la CEDEAO en date du 23 Mai 2009;

PRESCRIT :

CHAPITRE I

DISPOSITIONS GENERALES

Article Premier:

Définitions

Au sens de la présente Directive, les expressions ci-dessous sont définies comme suit:

communication électronique : toute mise à disposition au public ou à une catégorie du public par un procédé de communication électronique ou magnétique, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature ;

données informatiques : toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique ;

raciste et xénophobe en matière de TIC : tout écrit, toute image ou toute autre représentation d'idées ou de théories qui préconise ou encourage la haine, la discrimination ou la violence contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance, de l'affiliation ou de l'origine nationale ou ethnique ou de la religion, dans la mesure où cette dernière sert de prétexte à l'un ou à l'autre de ces éléments ou incite à de tels actes ;

mineur : toute personne âgée de moins de dix huit (18) ans au sens de la Convention des Nations Unies sur les droits de l'enfant ;

pornographie infantile : toute donnée quelle qu'en soit la nature ou la forme représentant de manière visuelle un mineur se livrant à un agissement sexuellement explicite ou des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite ;

système informatique: tout dispositif isolé ou non, tout ensemble de dispositifs interconnectés assurant en tout ou partie, un traitement automatisé de données en exécution d'un programme.

Technologies de l'information et de la communication (TIC) : technologies employées pour recueillir, stocker, utiliser et envoyer des informations et incluant celles qui impliquent l'utilisation des ordinateurs ou de tout système de communication y compris de télécommunication.

Article 2.

Objet

La présente Directive a pour objet d'adapter le droit pénal de fond et la procédure pénale des Etats Membres de la CEDEAO au phénomène de la cybercriminalité.

Article 3 :

Champ d'application

La présente Directive s'applique à toutes les infractions relatives à la cybercriminalité dans l'espace CEDEAO, ainsi qu'à toutes les infractions pénales dont la constatation requiert la collecte d'une preuve électronique.

CHAPITRE II:

INFRACTIONS SPECIFIQUES AUX TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Constituent des infractions au sens de la présente Directive :

Article 4:

Accès frauduleux à un système informatique

Le fait pour toute personne d'accéder ou de tenter d'accéder frauduleusement à tout ou partie d'un système informatique.

Article 5:

Maintien frauduleux dans un système informatique

Le fait pour toute personne de se maintenir ou de tenter de se maintenir frauduleusement dans tout ou partie d'un système informatique.

Article 6:

Entrave au fonctionnement d'un système informatique

Le fait pour toute personne d'entraver, de fausser, de tenter d'entraver ou de fausser le fonctionnement d'un système informatique.

Article 7:

Introduction frauduleuse de données dans un système informatique

Le fait pour toute personne d'introduire ou ***de*** tenter d'introduire frauduleusement des données dans un système informatique.

Article 8:

Interception frauduleuse de données informatiques

Le fait pour toute personne d'intercepter ou de tenter d'intercepter frauduleusement par des moyens techniques des données informatiques lors de leur transmission non publique à destination, en provenance ou à l'intérieur d'un système informatique.

Article 9:

Modification frauduleuse de données informatiques

Le fait pour toute personne d'endommager ou de tenter d'endommager, d'effacer ou tenter d'effacer, de détériorer ou de tenter de détériorer, d'altérer ou de tenter d'altérer, de modifier ou de tenter de modifier frauduleusement des données informatiques.

Article 10:

Falsification de données informatiques

Le fait pour toute personne de produire ou de fabriquer un ensemble de données numérisées par l'introduction, la suppression ou l'effacement frauduleux de données informatiques stockées, traitées ou transmises par un système informatique, engendrant des données contrefaites, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient originales.

Article 11:

Fraude informatique

Le fait pour toute personne d'obtenir frauduleusement, pour soi-même ou pour autrui, un avantage matériel ou économique par l'introduction, l'altération, l'effacement ou la suppression de données informatiques ou par toute forme d'atteinte au fonctionnement d'un système informatique.

Article 12:

Traitement frauduleux de données à caractère personnel

Le fait pour toute personne, même par négligence, de procéder ou faire procéder à des traitements de données à caractère personnel sans avoir respecté les formalités préalables à leur mise en œuvre telles que prescrites par la loi sur les données à caractère personnel prévue à cet effet dans chaque Etat Membre.

Article13:

Usage de données falsifiées

Le fait pour toute personne, en connaissance de cause, de faire usage de données falsifiées.

Article 14:

Disposition d'un équipement pour commettre des infractions

Le fait pour toute personne, sans motif légitime de produire, de vendre, d'importer, de détenir, de diffuser, d'offrir, de céder ou de mettre à disposition un équipement, un programme informatique, tout dispositif, donnée, un mot de passe, un code d'accès ou des données informatiques similaires adaptées pour commettre des infractions telles que définies par la présente Directive

Article 15:

Participation à une association formée ou à une entente en vue de commettre des infractions informatiques

Le fait pour toute personne de participer à une association formée ou à une entente établie en vue de préparer ou de commettre une ou plusieurs des infractions prévues dans la présente Directive.

Article 16

Production d'une image ou d'une représentation à caractère pornographique infantile

Le fait pour toute personne de produire, ***d'***enregistrer, ***d'***offrir, de mettre à disposition, de diffuser, de transmettre une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système informatique.

Article 17:

Importation ou exportation d'une image ou d'une représentation à caractère pornographique infantile

Le fait pour toute personne de se procurer ou de procurer à autrui, d'importer ou de faire importer, d'exporter ou de faire exporter une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système informatique.

Article 18:

Possession d'une image ou d'une représentation à caractère pornographique infantile

Le fait pour toute personne de posséder une image ou une représentation présentant un caractère de pornographie infantile dans un système informatique ou dans un moyen quelconque de stockage de données informatiques.

Article 19:

Facilitation d'accès à des images, des documents, du son ou une représentation présentant un caractère de pornographie à un mineur

Le fait pour toute personne de faciliter l'accès à des images, des documents, du son ou une représentation présentant un caractère de pornographie à un mineur.

Article 20:

Disposition d'écrits ou d'images de nature raciste ou xénophobe par le biais d'un système informatique

Le fait pour toute personne de créer, de télécharger, de diffuser ou de mettre à disposition sous quelque forme que ce soit des écrits, des messages, des photos, dessins ou toute autre représentation d'idées ou de théories, de nature raciste ou xénophobe, par le biais d'un système informatique.

Article 21:

Menace par le biais d'un système informatique

Toute menace commise par le biais d'un système informatique, de commettre une infraction pénale, envers une personne en raison de

son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance, la filiation, la religion, l'origine nationale ou ethnique, dans la mesure où cette appartenance sert de prétexte à une telle menace.

Article 22:

Injure commise par le biais d'un système informatique

Toute injure commise par le biais d'un système informatique envers une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance, l'origine nationale ou ethnique, la religion, la filiation dans la mesure où cette appartenance sert de prétexte à une telle injure.

Article 23:

Négationnisme

Tout fait intentionnel de nier, d'approuver ou de justifier par le biais d'un système informatique, des actes constitutifs de génocide ou de crimes contre l'humanité .

CHAPITRE III:

ADAPTATION DES INFRACTIONS CLASSIQUES AUX TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Article 24:

Circonstances aggravantes

Le fait d'utiliser les TIC ou d'agir en bande organisée en vue de commettre des infractions de droit commun comme le vol, l'escroquerie, le recel, l'abus de confiance, l'extorsion de fonds, le

terrorisme, le blanchiment de capitaux constitue une circonstance aggravante de ces infractions au sens de la présente Directive.

Article 25:

Atteinte portant sur les logiciels et programmes informatiques

Constitue une infraction, au sens de la présente Directive, le fait de commettre un vol, une, escroquerie, un recel, un abus de confiance, une extorsion de fonds, un acte de terrorisme, ou une contrefaçon portant les données informatiques, les logiciels et les programmes.

Article 26:

Infractions de presse commises *par des moyens de* communication électronique

Les infractions de presse commises par un moyen de communication électronique au sens de la présente Directive, sont soumises aux dispositions relatives aux infractions de presse applicables dans les Etats membres.

Article 27:

Responsabilité pénale des personnes morales autres que publiques

Toute personne morale à l'exception de l'Etat, des collectivités locales et des établissements publics, est tenue pour responsable des infractions prévues par la présente Directive, lorsqu'elles sont commises pour son compte par ses représentants. La responsabilité des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits.

CHAPITRE IV:

SANCTIONS

Article 28:

Peines principales

1. Les Etats membres sanctionnent les faits infractionnels prévus par la présente Directive. Les sanctions sont proportionnées et dissuasives.

2. Toute personne morale déclarée responsable au sens de la présente Directive, est passible de peines proportionnées et dissuasives, qui comprennent des amendes pénales et civiles.

Article 29:

Peines complémentaires

1. En cas de condamnation pour une infraction commise par le biais d'un support de communication électronique, la juridiction de jugement compétente peut prononcer des peines complémentaires.

2. En cas de condamnation, la juridiction compétente peut prononcer la confiscation des matériels, des équipements, des instruments, des programmes informatiques ou *des* données ainsi que des sommes ou produits résultant de l'infraction et appartenant au condamné.

3. Les décisions de condamnation sont publiées dans le journal officiel des Etats membres et sur un support électronique aux frais du condamné.

CHAPITRE V:

REGLES DE PROCEDURE

Article 30:

Perquisition ou accès à un système informatique

Les autorités nationales compétentes peuvent opérer des perquisitions ou saisies ou accéder à tout système informatique pour la manifestation de la vérité

Toutefois, lorsque la saisie du support électronique ne paraît pas souhaitable, les données, de même que celles qui sont nécessaires à la compréhension du système, font l'objet de copies sur des supports de stockage informatique et sont placés sous scellés.

Article 31

Conservation rapide des données informatiques archivées

Si les nécessités de l'information l'exigent et lorsqu'il y a des raisons de craindre la disparition des données informatiques archivées valant preuve, l'autorité compétente fait injonction à toute personne de conserver et de protéger dans le secret l'intégrité des données en sa possession ou sous son contrôle, dans un délai déterminé par chaque Etat membre.

Article 32

Mode de preuve:

L'écrit électronique est admis comme preuve en matière d'infraction à condition que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité.

Article 33

Coopération judiciaire

1. Lorsqu'ils sont saisis par un autre Etat membre, les Etats membres doivent coopérer à la recherche et à la constatation de toutes les infractions pénales prévues ou définies par la présente Directive ainsi qu'à la collecte de preuves sous forme électronique se rapportant à une infraction pénale.

2. Cette coopération est mise en œuvre dans le respect des instruments internationaux pertinents et des mécanismes sur la coopération internationale en matière pénale.

CHAPITRE VI:

DISPOSITIONS FINALES

Article 34:

Publication

La présente Directive sera publiée par la Commission dans le Journal Officiel de la Communauté dans les trente (30) jours de sa date de signature par le Président du Conseil des Ministres. Il sera également publié par chaque Etat Membre, dans son Journal Officiel trente (30) jours après que la Commission le lui notifiera.

Article 35 :

Mise en œuvre

1. Les Etats Membres adoptent les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente Directive au plus tard le 1er janvier 2014.

2. Lorsque les Etats Membres adoptent les dispositions visées au paragraphe 1 du présent article, celles-ci contiennent une référence à la présente Directive ou sont accompagnées d'une telle référence lors de leur publication officielle.

3. Les Etats Membres communiquent à la Commission de la CEDEAO les mesures ou dispositions qu'ils adoptent pour se conformer à la présente Directive.

4. Les Etats Membres de la Communauté notifient les difficultés de mise en œuvre de la présente Directive au Président de la Commission qui en fait rapport au Conseil des Ministres, qui, à son tour, prend les mesures appropriées en vue d'assurer la mise en œuvre effective de la présente Directive.

FAIT A ABUJA, LE 19 AOUT 2011

POUR LE CONSEIL,

LE PRESIDENT,

……
S.E. OLUGBENGA ASHIRU