NATIONS UNIES
COMMISSION ECONOMIQUE POUR L'AFRIQUE
Bureau Sous Régional pour l'Afrique Centrale

Union Internationale des Télécommunication

ATELIER COMMUN CEA-UIT SUR LA CYBERSECURITE ET LA CYBERCRIMINALITE
Libreville (Gabon) 28 novembre – 02 décembre 2011

RAPPORT FINAL

Libreville, 28 novembre au 2 décembre 2011

I. Introduction

Un atelier sur l'harmonisation du cadre légal pour la cybersécurité en Afrique Centrale, organisé par le Bureau Sous-régional pour l'Afrique centrale de la Commission Economique des Nations Unies pour l'Afrique (CEA/BSR-AC) en collaboration avec l'Union Internationale des Télécommunications (UIT) dans le cadre du projet HIPSSA, la CEEAC et la CEMAC s'est tenu à Libreville (Gabon) du 28 novembre au 02 décembre 2011.

Cet atelier fait suite à la deuxième réunion des Ministres en charge des Télécommunications et TIC des Etats membres de la CEEAC tenue à Ndjamena, le 22 avril 2010 qui a recommandé au Conseil statutaire des Ministres de la CEEAC, de soumettre à l'approbation de la Conférence des Chefs d'Etats et de Gouvernement de la CEEAC. Cette demande avait d'ailleurs fait l'objet d'une recommandation lors du Conseil des Ministres de la CEMAC en décembre 2008.

Afin d'assister le Secrétariat Général de la CEEAC et la Commission de la CEMAC dans l'exécution de ces recommandations, l'UIT et la CEA ont proposé de développer conjointement un cadre juridique régional harmonisé qui prendra des formes différentes pour chacune de ces deux organisations, en fonction de leurs instruments juridiques respectifs (directives et/ou règlements pour la CEMAC et lois-types et/ou lignes directrices pour la CEEAC).

II. Participation

Ont pris part aux travaux, les experts des Etats membres de la CEEAC et de la CEMAC, à savoir : l'Angola, le Burundi, le Cameroun, le Congo, le Gabon, la Guinée Equatoriale, la République Centrafricaine, la République Démocratique du Congo (RDC), Sao Tomé et Principe et le Tchad.

Les délégations des Etats membres étaient composées de plusieurs Experts, notamment les parlementaires, les représentants des ministères en charge des TIC, de la justice, de l'économie et du commerce, de la sécurité, de l'intégration régionale, des agences et opérateurs du secteur des TIC et de la Société Civile.

Étaient également représentées à cette réunion, les organisations internationales suivantes : l'Union Africaine, la Communauté Economique des Etats de l'Afrique Centrale (CEEAC), la Communauté Economique et Monétaire de l'Afrique Centrale (CEMAC), le Bureau sous régional d'Interpol, la CEA, l'UIT et la CNUDCI.

La liste des participants est jointe en annexe I du présent rapport.

III. Cérémonie d'ouverture

La cérémonie d'ouverture a été présidée par S.E. M. **Aurélien NTOUTOUME**, Ministre des Relations avec le Parlement et les Institutions Constitutionnelles, de l'Intégration Régionale et du NEPAD, chargé des Droits de l'Homme de la République Gabonaise, représentant S.E. M. **Paul NDONG NGUEMA,** Ministre de la Communication, de la Poste et de l'Economie Numérique en mission.

Cette cérémonie a été ponctuée par six discours, à savoir, celui de la CEA, de la CEMAC, de l'UIT, de l'UA, de la CEEAC et du Ministre gabonais en charge des Télécommunications.

Prenant la parole pour le compte de la CEA, M. **Emile AHOHE**, Directeur du Bureau Sous Régional de la CEA pour l'Afrique Centrale (CEA/BSR-AC), a estimé que la Cybercriminalité dans les pays où elle se développe, génère une image négative et elle dissuade les investisseurs potentiels, créateurs de richesse et d'emplois. A cet effet, la coopération policière et judicaire internationale doit être une priorité absolue, compte tenu de l'absence de frontières physiques du cyberespace.

Intervenant au nom du Président de la Commission de la CEMAC, M. **Isidore EMBOLA** a souhaité que les Télécommunications, les Technologies de l'Information et de la Communication (TIC), qui constituent des supports et des facilitateurs du développement économique, social et culturel, fassent l'objet d'une attention particulière au niveau des Etats, notamment la cybersécurité et cybercriminalité.

De son coté M. **Jean-Jacques MASSIMA LANDJI**, Représentant de l'UIT pour l'Afrique Centrale et Madagascar, a dans son discours, déclaré qu'un cadre légal harmonisé où tous les maillons sont constitués d'anneaux de pur métal, permet d'avoir une réponse solide et cohérente à l'assainissement du Cyberespace et à l'édification d'une société de l'Information inclusive et juste permettant à tous de bénéficier des mêmes opportunités et cela en Toute Sécurité !

Pour le Représentant de la Commission de l'Union Africaine (CUA) **M. Moctar YEDALY**, la Convention de l'Union Africaine est plus que nécessaire, voire vitale, pour inspirer les états membres et leurs législateurs sur les questions de cybersécurité, de cybercriminalité et de protection des données à caractère personnel.

S.E. Général **Louis SYLVAIN-GOMA**, Secrétaire Général de la CEEAC a quant à lui, déclaré qu'il est illusoire d'engager le développement du gouvernement en ligne, du commerce en ligne et de la santé en ligne, si rien n'est envisagé sur les aspects juridiques, organisationnels, humains et technologiques de la sécurité de réseaux et de l'information.

Dans le discours d'ouverture, le Ministre des Relations avec le Parlement et les Institutions Constitutionnelles, de l'Intégration Régionale et du NEPAD, chargé des Droits de l'Homme de la République Gabonaise, a d'une part, souhaité la bienvenue à l'ensemble des délégués, et a d'autre part, invité les Experts en télécommunications, les Juristes, les Parlementaires, les membres des forces de sécurité et autres acteurs du secteur de la cybersécurité en Afrique Centrale à proposer une vision et des textes communautaires de référence sur la cybersécurité dans la sous-région, qui seront transposés dans les dispositifs nationaux des Etats membres. Il a exhorté les

délégués au travail afin de doter la sous-région d'un cadre juridique propice pour la lutte contre la cybercriminalité.

L'ensemble des discours sont joints en annexe 2.

IV. Mise en place du bureau

Après la cérémonie d'ouverture, les Experts des Etats membres de la CEEAC et de la CEMAC ont mis en place un bureau composé ainsi qu'il suit :

Présidence :	Mme **Florence LENGOUMBI KOUYA**	(Gabon)
Vice-présidence :	M **Abdoul HAMZA BOUKAR**	(Tchad)
Rapporteur :	M **Guy Roland NTSIMBA**	(République du Congo)
Vice Rapporteur :	M **Sabin NIKOYAGIZE**	(Burundi)

V. Adoption de l'ordre du jour et du programme de travail

Les Experts ont adopté l'ordre du jour de l'atelier ainsi que le programme de travail (cf. annexe 3). Les points ci-dessous ont été examinés :

1. Présentation du rapport « La Cybercriminalité : une guerre numérique et sournoise » ;
2. Présentation de la politique cadre et initiative de la CEA pour l'harmonisation des cyber-législations en Afrique ;
3. Présentation du programme d'action du projet HIPSSA commun UIT-CE pour l'Afrique centrale ;
4. Présentation des textes de la CNUDCI sur les transactions électroniques ;
5. Présentation des actions d'INTERPOL en matière de coopération internationale ;
6. Présentation et définition des terminologies : Cybersécurité et cybercriminalité ;
7. Présentation de l'expérience de la CEDEAO en matière d'harmonisation des cyber-législations en Afrique de l'Ouest ;
8. Présentation du projet de Convention de l'Union Africaine sur la mise en place d'un cadre juridique de confiance pour la cybersécurité en Afrique ;
9. Examen des avant-projets de directive CEMAC et de loi-type CEEAC sur les transactions électroniques ;
10. Examen des avant-projets de directive CEMAC et de loi-type CEEAC sur la protection des données personnelles ;
11. Examen des avant-projets de directive CEMAC et de loi-type CEEAC sur les transactions électroniques ;

a K

12. Examen des avant-projets de directive CEMAC et de loi-type CEEAC sur la lutte contre la cybercriminalité ;
13. Actions futures.

VI. Déroulement des travaux et résultats

Les travaux se sont déroulés en sessions plénières. Les différents points inscrits à l'ordre du jour ont fait l'objet de présentations suivies de débats et de recommandations formulées par les participants.

1. Présentation du dossier intitulé « La Cybercriminalité : une guerre numérique et sournoise ».

Le Bureau Sous-régional pour l'Afrique Centrale de la CEA a présenté le rapport sur la Cybercriminalité préparé pour la réunion. La présentation composée de 5 parties, avait pour objet de faire un état des lieux de la cybercriminalité et cybersécurité tant au plan économique que politique, et d'en expliquer les principales problématiques. La première partie a exposé une définition de la cybercriminalité et présenté les actions de malveillances que l'on peut qualifier de cyberdélits (vol d'identité, piratage informatique...). La seconde partie a montré les effets de la cybercriminalité sur l'économie mondiale, la troisième et quatrième partie de l'exposé ont mis en exergue les conséquences des menaces des cybers attaques sur la paix et la sécurité au niveau mondial, en soulignant l'absence d'un cadre légal international pour lutter contre ce fléau. La dernière partie a fait l'objet de recommandations et de propositions en indiquant quelques pistes de réflexion pour minimiser les risques et accroître la coopération internationale.

La présentation a été suivie de débats et de discussions au cours desquels les participants ont formulé des observations, des commentaires et des amendements qui permettront d'améliorer le contenu du rapport d'étude. Les participants ont également formulé des recommandations additionnelles qui seront intégrées dans le rapport final de l'étude.

2. Présentation de la politique cadre et initiative de la CEA pour l'harmonisation des cyberlégislations en Afrique.

Cette présentation a été faite conjointement par Madame **Eskedar Nega**, chargée de programme TIC et de Monsieur **Mohamed TIMOULALI**, conseiller régional TIC, tous deux de la Commission Economique des Nations Unies pour l'Afrique. Elle avait pour objet d'informer les Experts sur le cadre de l'initiative de la société de l'information en Afrique, comme vision régionale du continent adoptée en 1996, et des actions entreprises au plan national et continental.

Grâce à ce cadre de référence régional, plus de 35 pays africains et les Communautés Economiques Régionales (CER), se sont à ce jour respectivement

RK

dotés de plans d'infrastructures nationaux des TIC et des cyberstratégies sectorielles qui donnent l'orientation politique et stratégique permettant la promotion d'une société de l'information inclusive à travers divers outils tels que les cadres juridiques et réglementaires, l'identification d'applications sectorielles en fonction des priorités économiques et sociales des pays, la promotion des contenus locaux ainsi que des activités de renforcement des capacités ciblant un large éventail de parties prenantes.

Cette présentation a été conclue sur l'importance d'ancrer les efforts de formulation de cyber-législations en complément d'autres initiatives en amont ayant pour objectif principal de mettre en place un environnement politique et juridique propice au déploiement des TICS au service du développement.

3. Présentation du programme d'action du projet HIPSSA commun UIT-CE pour l'Afrique centrale.

Le représentant de l'UIT pour la zone Afrique centrale et Madagascar a présenté les actions menées par l'UIT comme agence d'exécution dans le cadre du projet HIPSSA, financé par l'Union Européenne et coordonné par l'Union Africaine. Ce projet s'exerce dans le contexte de soutien au développement de politiques harmonisées et d'environnements réglementaires pour les TIC efficaces, propices aux investissements massifs requis par les infrastructures et les applications des TIC dans les pays ACP.

L'atelier sur la cybersecurité organisé conjointement avec la CEA pour les pays de l'Afrique Centrale complète le dispositif mis en place de manière harmonisée relative aux lois institutionnelles dans le secteur des TIC et aux appuis nécessaires de renforcement des capacités relatives aux domaines suivants : octroi de licences, gestion des ressources rares (gestion du spectre, plan de numérotation), interconnexion, migration vers la TV numérique, statistiques et Indicateurs.

Les recommandations issues de l'étude comparative menée dans les sous régions peuvent se résumer ainsi :

- trois étapes d'harmonisation nécessaires (Panafricain, Régional, National)
- réduire le niveau de disparité réglementaire au niveau national et régional en se basant sur une plateforme commune pour toutes les organisations régionales
- renforcer un instrument panafricain commun afin de garantir : l'objectivité, la transparence, la proportionnalité, la non-discrimination etc.

Le projet HIPPSSA, suite à l'harmonisation des textes prévoit d'assister les pays dans la transposition des lois-types, des directives dans les pays respectifs en collaboration avec la CEMAC et la CEEAC.

Par ailleurs, il a vivement recommandé une collaboration plus étroite entre les différentes CER afin de simplifier les cadres normatifs de référence et de faciliter le suivi et l'évaluation des mesures prises et des progrès réalisés.

4. Présentation des textes de la CNUDCI sur les transactions électroniques.

Le Professeur **Etienne MONTERO**, intervenant au nom de la Commission des Nations Unies pour le Droit Commercial International (CNUDCI), a fait une présentation des textes de la CNUDCI sur les transactions électroniques. Après avoir fourni quelques données statistiques sur la réalité du commerce électronique dans le monde et expliqué quelques notions de base (réseaux fermés et réseaux ouverts, différentes relations telles que B2B, B2C, C2C, G2B, G2G et C2G), il a fait état des obstacles juridiques liés au commerce électronique.

Ensuite, l'orateur s'est attaché à exposer les grands principes régulateurs à la base des textes de la CNUDCI : *le principe de non-discrimination, le principe d'équivalence fonctionnelle* et *le principe de neutralité technologique*. Il a illustré son propos en commentant les dispositions relatives à l'écrit, à l'original et à la signature dans les textes de la CNUDCI.

5. Présentation des actions d'INTERPOL en matière de coopération internationale.

M. **Marcel Yves MAPANGOU-MOUSSADJI**, officier spécialisé au bureau régional INTERPOL pour l'Afrique Centrale, après un bref aperçu historique de l'organisation, a d'une part, présenté le rôle de l'Organisation Internationale de Police Criminelle (OIPC-Interpol) dans la coopération policière internationale et d'autre part, décrit les compétences de l'organisation dans la coordination des enquêtes internationales avant de faire état des outils développés par INTERPOL et mis à la disposition des pays membres.

Au cours de son exposé, l'officier a fait état de la nécessité de renforcer les capacités des acteurs de première ligne et la mutualisation des efforts pour combattre le phénomène.

En guise de conclusion, il a formulé le vœu de voir les pays s'atteler à établir une cartographie de cette forme de criminalité, tout en faisant l'effort de rayer la carence juridique et technologique qui profite aux malfaiteurs. En réponse à la préoccupation d'un délégué, l'officier a rassuré l'assistance sur la réalité de la coopération entre les services chargés de l'application de la loi au sein du comité des chefs de police de l'Afrique centrale (CCPAC), organe spécialisé de la CEMAC, et a noté avec satisfaction les progrès réalisés par les FAI au regard des mesures d'identification préalable et obligatoire des usagers de téléphonie mobile lors de l'achat d'une carte SIM dans de nombreux pays de la sous région.

6. Présentation et définition des terminologies : Cybersécurité et cybercriminalité.

Le Professeur **Abdoullah Cissé**, expert en légistique et en cyberdroit a insisté sur l'importance de l'harmonisation de la terminologie et des définitions dans un environnement marqué par la diversité des cultures juridiques et par la diversité linguistique.

De son intervention, il est ressorti la différence entre la cybercriminalité et la cybersécurité comme résultante de la place accordée respectivement d'une part à la sécurité comme objectif d'ordre public primordial dans le cyberespace et d'autre part, à la criminalité comme atteinte majeure dans le cyberespace.

La cybersécurité en raison de ses multiples dimensions (technologique, juridique, sociétale, économique, psychologique etc.) part d'une approche holistique, globale et englobe deux séries de questions :

- D'un côté, les questions relevant directement de la cybersécurité tels la sécurité des réseaux et des infrastructures, l'échange de données informatisées, le cadre institutionnel, la coopération internationale, la normalisation etc.
- D'un autre côté, les questions en relation avec la cybersécurité mais relevant de matières comme les transactions électroniques y compris la preuve et le commerce électroniques, la protection des données à caractère personnel, la lutte contre la cybercriminalité, la propriété intellectuelle, les télécommunications etc.

La cybersécurité peut être appréhendée au moyen d'une approche pluridisciplinaire englobant les deux dimensions ou bien au moyen d'une approche monodisciplinaire limitée à une dimension ou une matière.

La cybercriminalité quant à elle part d'une approche sectorielle de droit pénal ou de politique criminelle et est traitée par voie de conséquence à partir d'une perspective juridique. Elle englobe les questions de droit pénal et de procédure pénale ainsi que celles liées à la coopération policière et judiciaire.

Fort de cette distinction, il a recommandé qu'une option soit faite par les Etats sur la signification qu'ils veulent privilégier pour servir de base à l'harmonisation terminologique. Dans cette perspective, il est nécessaire de :

- Utiliser les mêmes termes pour exprimer les mêmes concepts ;
- Recenser et analyser les définitions consacrées dans les Etats membres, les CER et celles révélées par la pratique internationale ;
- Choisir les termes à définir et stabiliser la liste des termes à définir dans les textes juridiques à élaborer ;
- Harmoniser les définitions dans le respect du principe de la neutralité technologique ;
- Veiller à l'articulation cohérente entre les définitions consacrées et le contenu des normes posées ou à poser.

7. Présentation de l'expérience de la CEDEAO en matière d'harmonisation des cyber-législations en Afrique de l'Ouest.

Le Professeur **CISSE** a présenté le processus d'harmonisation qui a été initié dans l'espace UEMOA-CEDEAO au titre du partage d'expérience entre les CER. Il a insisté sur la démarche, les étapes et les résultats obtenus à savoir l'adoption en 2010 de deux actes additionnels portant respectivement sur la protection des données à caractère personnel et les transactions électroniques. Le projet de directive portant

sur la lutte contre la cybercriminalité est quant à lui en cours d'adoption. Il est à noter que les textes de la CEDEAO ne traitent pas des questions relevant strictement de la cybersécurité et qui sont consacrées dans l'avant-projet de Convention de l'Union africaine.

8. Présentation du projet de convention de l'Union Africaine sur la mise en place d'un cadre juridique de confiance pour la cybersécurité en Afrique.

Le Représentant de la Commission de l'UA, en guise d'introduction à la présentation du Professeur CISSE, a rappelé :

- La vision de l'Union Africaine, à savoir : *« Construire une Afrique intégrée, en paix, prospère, dirigée par ses propres citoyens et représentant une force dynamique dans l'arène internationale »*. C'est dans ce cadre que l'Action de la Commission de l'UA vise la création d'un environnement favorable pour le marché des TIC. En un mot son agenda continental est axé sur : Les mesures légales, techniques et procédurales, les structures organisationnelles, le renforcement des capacités, la coopération internationale et continentale.

- Qu'en mai 2008, la deuxième Conférence des Ministres en charge des TIC a adopté un cadre de référence pour l'Harmonisation des politiques et régulations des TICs en Afrique.

- Que c'est en décembre 2009, lors de leurs Conférence Extraordinaire que les Ministres de l'Union Africaine en charge des TIC ont demandé à la Commission de l'UA de développer conjointement avec la CEA une convention sur la cyber-législation répondant aux besoins du continent et qui adhère aux demandes légales et réglementaires des transactions électroniques, la cybersécurité et la protection des données à caractère personnel. Il a été recommandé que cette convention soit adoptée par les Etats membres de l'UA en 2012.

L'objectif est de coordonner toutes ces actions afin d'éviter une cacophonie juridique, la duplication des efforts et la perte des ressources. Il est à noter que la CEA et la Commission de l'UA sont mandatées pour préparer et présenter ladite convention pour adoption aux Etats membres. De même, cette convention devrait être inclusive et former le chapeau général, la référence pour toute action entreprise ou à entreprendre dans la cadre de la cyber-sécurité afin de faciliter l'harmonisation et l'Intégration Régionale.

Le Professeur **CISSE** a par la suite, présenté le cadre de référence méthodologique élaboré par la CEA comme outil de facilitation des processus d'harmonisation régionale des cyberlégislations.
Il part du contexte continental et sous régional pour présenter les principales références textuelles des organisations régionales pour fonder la légitimité et la nécessité d'une telle démarche et la complémentarité entre les organisations intervenantes.

Dans un premier temps, il a évoqué la démarche d'harmonisation en mettant l'accent sur les principales étapes de la démarche de légistique à savoir :

- le cyberaudit juridique qui permet de faire l'état des lieux et d'identifier les problèmes à étudier :
- le benchmark qui permet de recenser les bonnes pratiques internationales, régionales et nationales ;
- la cyberstratégie qui permet de fixer les orientations stratégiques des Etats et des organisations d'intégration ;
- la rédaction des avant-projets de textes en recherchant au préalable le support textuel le plus approprié en tenant compte des contraintes institutionnelles de chaque organisation (directives, règlement, acte additionnel, lignes directrices, loi-type etc.) ;
- les procédures d'adoption et de transposition des normes y compris la mise en harmonie avec les législations nationales et les questions de mise en œuvre.

Il a par ailleurs, évoqué les préceptes de légistique qui permettent de garantir la qualité rédactionnelle des textes en veillant notamment sur les questions de cohérence interne (le contenu des textes) et externe des textes proposés (articulation avec les normes internationales, régionales et nationales).

La finalité de la démarche est de parvenir à créer un environnement juridique de confiance qui soit prévisible, organisé, protecteur, sécurisé et intégré à l'ordre international.

9. Examen des avant-projets de directive CEMAC et de loi-type CEEAC sur les transactions électroniques ;

Le consultant HIPSSA, M **Hervé Jacquemin**, a d'abord, présenté brièvement la thématique des transactions électroniques. Il a insisté sur la nécessité de définir clairement le champ d'application de la loi type, d'un point de vue matériel, personnel et spatial, de consacrer les principes d'assimilation et de non-discrimination, tout en laissant aux parties la liberté de recourir ou non aux TIC dans les transactions électroniques. L'identification du prestataire est également cruciale. Il a insisté sur le fait que la publicité en ligne doit être réglée, pour garantir la transparence et la loyauté sur les réseaux, tout en interdisant, sous conditions, l'envoi de courriers électroniques publicitaires non sollicités. S'agissant de la conclusion du contrat par voie électronique, une distinction est faite entre les réponses à apporter aux difficultés posées par l'utilisation des technologies de l'information et de la communication (dans les relations B2B et B2C), d'une part, par la distance qui sépare les parties (dans les relations B2C, uniquement), d'autre part. Le consultant a aussi souligné la nécessité de lever les obstacles à l'accomplissement des règles de forme par voie électronique, en consacrant notamment la théorie des équivalents fonctionnels et le principe de neutralité technologique. Enfin, il a exposé les raisons pour lesquelles certains prestataires intermédiaires devraient bénéficier d'une exonération de responsabilité et insisté sur l'importance de prévoir des sanctions civiles et pénales effectives, dissuasives et proportionnées, en cas de violation des dispositions de la loi.

Ensuite un état des lieux des législations nationales a été fait par Me **SARR**. Il en ressort que la tentative de collecte des données auprès des régulateurs et des personnes ressources dans la zone d'étude a permis de constater la quasi absence de législations relatives au commerce électronique. Certes, dans l'ensemble des deux zones communautaires, des stratégies nationales de TIC ont été élaborées ainsi que les politiques intégrant la réforme des cadres législatifs et réglementaires. Mais lorsque ces initiatives existent, elles ne sont pas toujours suivies d'une mise en œuvre effective. Par ailleurs, dans les politiques TIC existantes au sein de chacun des dix pays, l'approche donnée aux instruments législatifs nationaux et même régionaux est une approche « télécoms » qui n'intègre que les grandes questions et principes en matière de télécommunications.

L'audit régional institutionnel réalisé, a permis d'identifier des dispositifs législatifs régionaux (OHADA, CEMAC) qui peuvent dans une certaine mesure suppléer l'absence de textes dans la zone concernée.

En outre, le consultant de l'HIPSSA a rappelé qu'il s'est principalement fondé sur l'avant-projet de la Convention de l'Union africaine sur la cybersécurité, l'acte additionnel de la CEDEAO, l'acte uniforme de l'OHADA portant sur le droit commercial général, ainsi que les textes de la CNUDCI et de l'Union européenne pour la rédaction de ces avant-projets.

Il a enfin, présenté brièvement les éléments-clés de la loi type/directive, en examinant successivement le champ d'application et les définitions ; les principes fondamentaux ; l'obligation générale d'information ; la publicité en ligne ; la conclusion des contrats par voie électronique ; la responsabilité des prestataires intermédiaires ; les sanctions ainsi que les codes de conduite et la mise en place de règlements extrajudiciaires des litiges.

Il sied de souligner que cette présentation a suscité un débat, au cours duquel, les délégués ont décidé unanimement de remplacer l'intitulé du projet de loi type (initialement, loi type sur le commerce électronique), de sorte qu'il devienne *« loi type sur les transactions électroniques »,* et ce conformément aux termes de référence. Ils ont ensuite recommandé de modifier la structure de l'avant-projet de texte, de sorte que celui-ci reflète clairement les aspects juridiques des transactions électroniques, comprenant le commerce électronique et la signature électronique, tels qu'ils figurent dans le projet de Convention de l'Union africaine.

10. Examen des avant-projets de directive CEMAC et de loi-type CEEAC sur la protection des données à caractère personnel.

Les consultants HIPSSA ont exposé les enjeux de la thématique en insistant sur la nécessité de prévoir des règles uniformes de protection des données à caractère personnel dans une région donnée.

Ils ont insisté sur, d'une part, les dimensions humaines de la thématique tenant dans les droits fondamentaux de l'Homme et, d'autre part, les risques qui surgissent dans l'explosion des Technologies de l'Information et de la Communication tels que le risque d'affaiblissement de la protection des données à caractère personnel.

Les consultants ont, dans le cadre de leur mission, travaillé sur un état des lieux tant national, régional, qu'international, et se sont basés sur le projet de Convention de l'Union Africaine relative à la mise en place d'un cadre juridique de confiance pour la cybersécurite en Afrique, les textes de la CEMAC/CEEAC/CEDAO/OHADA, les textes de l'Union Européenne, de l'ONU, de l'OCDE ainsi que les textes nationaux.

Au terme de l'analyse, les consultants ont dégagé des principes qui sont récurrents dans les divers règlements internationaux afin de pouvoir les prendre en compte lors de la rédaction de la loi-type. Il s'agit de ceux de transparence, de définitions, de détermination des finalités, de légitimité, de nécessité/proportionnalité, de qualité des données, de données particulières, sécurité, de confidentialité, de droits de la personne concernée, de sanction, d'autorité de contrôle/protection et de flux transfrontières.

Les consultants ont également rappelé que la loi-type n'avait pas, pour objectif, de se substituer à des lois nationales mais à offrir une référence en vue d'une harmonisation des lois nationales.

Suite à cette présentation, les Experts ont insisté sur le fait que le régime de protection des données à caractère personnel devrait nécessairement se fonder sur les cultures sociales, religieuses, politiques et régionales pour atteindre son objectif de protection et d'harmonisation.

Par ailleurs, ils ont rappelé la mise en place d'un régime de protection des données à caractère personnel ne sera effective qu'avec la création d'une autorité de protection qui devrait assurer une fonction de contrôle du bon respect de la législation et de la protection de la vie privée en général.

Cet avant-projet de textes a été adopté par les Experts, avec amendements.

11. Examen des avant-projets de directive CEMAC et de loi-type CEEAC sur la lutte contre la cybercriminalité.

Les consultants HIPSSA ont exposé les enjeux de la thématique portant sur la lutte contre la cybercriminalité. Le débat a été ouvert par la présentation des enjeux dans le domaine de la lutte contre la cybercriminalité, accompagné de l'état des lieux dans les Etats membres de la CEMAC et de la CEEAC.

Les consultants ont présenté la structure générale de la proposition de la loi-type sur la cybercriminalité et procédé à la lecture des concepts et des articles qui en découlent.

Le débat a porté sur l'intitulé du projet de loi type, au regard des termes de référence, à savoir « la lutte contre la cybercriminalité », les sanctions pénales, la définition et/ou l'adoption de certaines infractions nouvelles spécifiques aux TIC et l'adaptation des infractions classiques, telles que liées aux systèmes informatiques, les données la pornographie enfantine et les Spams.

Pour rendre effective la lutte contre la cybercriminalité, la politique de lutte criminelle devra intégrer la formation des acteurs, la sensibilisation des citoyens à la cybersécurité, le cadre institutionnel de lutte contre la cybercriminalité et la coopération (régionale, internationale), y compris la coordination des acteurs nationaux.

Par conséquent, les Experts ont demandé aux consultants de proposer un avant projet de loi-type sur la lutte contre la cybercriminalité qui intègre le texte sur la cybercriminalité examiné au cours de l'atelier, avec les amendements y relatifs et les aspects de la cybersécurité ci-dessus.

12. Actions futures du Secrétariat Général de la CEEAC et de la Commission de la CEMAC.

Les deux institutions sont revenues sur la méthodologie d'élaboration des lois types et des directives sur la cybersécurité (les transactions électroniques, la protection des données à caractère personnel et la lutte contre la cybercriminalité) ; elles ont précisé que compte tenu de l'importance de la coopération régionale et internationale en matière de cybersécurité et du fait qu'un seul pays de l'Afrique centrale dispose à ce jour d'une loi sur la cybersécurité, l'élaboration des instruments juridiques régionaux d'harmonisation des réglementations nationales sur la cybersécurité devraient s'inspirer de la convention des nations unies, des recommandations des institutions spécialisées des nations Unies et de la Convention de l'Union Africaine en la matière.

Elles ont indiqué que leurs programmes d'action respectifs pour l'année 2012 prévoient la tenue d'une réunion des ministres en charge des TIC en mars 2012.

Compte tenu du fait que le présent atelier n'a pas terminé l'examen des textes proposés, un deuxième atelier de validation des projets de lois types et directives se tiendra trois jours avant la réunion des Ministres. A cette fin, elles mettront tout en œuvre pour faire parvenir les projets de textes à examiner aux Etats membres au moins 15 jours avant la date de la tenue de ce deuxième atelier de validation.

Suite à cet exposé, le calendrier suivant a été adopté :

24 décembre 2011	Envoi des projets de lois types et directives par les consultants au Secrétariat général de la CEEAC et à la Commission de la CEMAC
30 décembre 2011	Envoi des projets de lois types et directives aux Etats membres par le Secrétariat général de la CEEAC et la Commission de la CEMAC
02 février 2012	Envoi des commentaires des Etats membres sur les textes proposés à la CEEAC et à la CEMAC
15 février 2012	Envoi des commentaires aux consultants par la CEEAC et la CEMAC
29 février 2012	Envoi des projets amendés par les consultants au Secrétariat général de la CEEAC et à la Commission de la CEMAC
05 mars 2012	Envois des projets amendés aux Etats membres

L'ensemble des présentations sont en annexe 4.

13. Recommandations

A la fin des travaux, les experts ont formulé les recommandations jointes en annexe 5.

14. Clôture de l'atelier

Les travaux des Experts ont été clôturés par **Mme Florence LENGOUMBI KOUYA,** représentant le Ministre de la Communication, de la Poste et de l'Economie Numérique de la République Gabonaise, qui s'est félicitée de la qualité des travaux et de la participation active des Experts atelier (Cf. annexe 7). Deux motions de remerciement ont été adressées respectivement à S.E. Monsieur le Président de la République Gabonaise et aux organisateurs dudit atelier (Cf. annexe 6).

Fait à Libreville, le 02 décembre 2011

Le Rapporteur

Guy Roland NTSIMBA

la Présidente

Florence LENGOUMBI KOUYA

ANNEXE 5

RECOMMANDATIONS

Les Experts sur l'harmonisation du cadre légal pour la cybersécurité et la cybercriminalité en Afrique centrale, réunis à Libreville, au Gabon du 28 novembre au 02 décembre 2011,

Considérant que les projets de lois types et directives doivent tenir compte d'une part des orientations régionales fixées par la CEEAC et la CEMAC, et d'autre part, de la nécessité de prendre en compte la coopération internationale, la sensibilisation et le renforcement des capacités des citoyens en matière de cybersécurité, formulent les recommandations suivantes :

Recommandation 1 :

Il est recommandé aux Etats membres de la CEEAC et de la CEMAC, de poursuivre la formulation et la mise en œuvre des politiques et stratégies nationales permettant une transition vers une société du savoir pérenne et inclusive, notamment par la création d'un environnement de confiance et de sécurité dans le domaine des TIC.

Recommandation 2 :

Il est recommandé à la Commission Economique des Nations Unies pour l'Afrique de continuer à soutenir les efforts de la Commission de l'Union Africaine dans la finalisation de l'avant-projet de convention de l'UA sur la cybersécurité.

Recommandation 3 :

Il est recommandé à la Commission Economique des Nations Unies pour l'Afrique et à l'Union Internationale des Télécommunications de continuer à soutenir les efforts de la CEEAC et la CEMAC dans la finalisation de leurs projets d'harmonisation des cadres réglementaires régionaux et nationaux sur la cybersécurité.

Recommandation 4 :

Il est recommandé aux Etats membres de la CEEAC et de la CEMAC, en partenariat avec l'UA, la CEA et l'UIT, de développer des programmes de renforcement de capacités qui faciliteront la transposition des lois types/directives sur les transactions électroniques, la protection des données à caractère personnel et la lutte contre la cybercriminalité.

Recommandation 5 :

Il est recommandé la création d'un groupe de travail composé de la CEA, l'UIT, la CEEAC et la CEMAC, chargé du suivi des travaux des consultants et de s'assurer, dans les délais requis, de la mise en conformité des documents suivant les recommandations des Experts et d'éditer un lexique des termes afférents à la cybersécurité.

Recommandation 6 :

Pour une meilleure harmonisation des textes régionaux, les experts recommandent que la CEEAC et la CEMAC tiennent compte de l'avant-projet de convention de l'UA sur la cybersécurité, lors de l'élaboration et de l'adoption respective des lois-types et des directives sur la lutte contre la cybercriminalité, les transactions électroniques et la protection des données à caractère personnel.

Recommandation 7 :

En vue de préparer le terrain à l'adoption des lois-types de la CEEAC et des directives de la CEMAC ainsi que de la Convention de l'UA sur la cybersécurité, les experts recommandent au Secrétariat général de la CEEAC, à la Commission de la CEMAC et aux Etats membres de mener une large consultation régionale et nationale en impliquant toutes les parties prenantes (Gouvernement, Parlement, secteur privé et société civile).

Recommandation 8 :

Pour améliorer l'avant-projet de Convention de l'UA sur la cyber sécurité, les experts recommandent aux Etats membres de faire parvenir au Secrétariat général de la CEEAC leurs observations sur cet avant-projet de convention avant le 31 décembre 2011. Le Secrétariat général de la CEEAC consolidera ces observations et les fera parvenir à la Commission de l'UA avant le 15 Janvier 2012.

Recommandation 9 :

Le secrétariat général de la CEEAC et la commission de la CEMAC sont invités à fournir les services d'interprétation lors des réunions et à traduire tous les documents dans les langues officielles de la Communauté (français, anglais, espagnol et portugais).