ACEH-Les Compagnons Solidaires

Action Terre d'Afrique

Association de Coopération et d'Entraide Humanitaire
Dotée du Statut Consultatif « Spécial » auprès du Conseil économique et social des Nations Unies depuis le 21juillet 2021
- 1 Square Paul Gauguin 95380 Louvres France.
- aceh.info.communication@gmail.com
- tél. +33 (0) 7 49 65 98 67
-tel. +237 699749425
- http://aceh-lescompagnonssolidaires.e-monsite.com
FB : https://www.facebook.com/ACEH-Lescompagnonssolidaires-ActionTerre dAfriaue/
Financée par le Ministère des affaires étrangères et du développement international.

Réseau multi-acteurs de coopération et de solidarité internationale, pour le Développement durable, l'éducation, formation, la santé, l'agriculture, pour la lutte contre la pauvreté, la faim, pour la protection de la nature et pour la lutte contre le réchauffement climatique.

ADRESSÉ À:

M. Marc-André Dorel
Acting Chief NGO Branch,
Office for ECOSOC Support and Coordination
DESA
United Nations New York 10017.

Louvres le, 24 Janvier 2022

Objet : Proposition de contribution ACEH-Compagnons Solidaires au Comité ad hoc pour l'élaboration d'une convention internationale globale sur la lutte contre l'utilisation des technologies de l'information et de la communication à des fins criminelles. Conformément à la résolution 74/247 de l'Assemblée générale des Nations Unies du 27 Décembre 2019.
Prévu le 17-28 Janvier 2022 et renvoyé à une date ultérieure.

- ONUDC -

Titre1.
De l'application de la loi pénale
Chapitre1
Dispositions préliminaires-Infractions,

Article1 : Cybercriminalité-usage malveillant du digital audiovisuel et de vidéogrammes sonores

1) Est considéré comme cybercriminalité, toute activité malveillante qui consiste à faire usage abusivement des outils modernes de technologies de l'information et de la communication (TIC) pour poser des actes haineux et criminels.

Article 2 : Cyber attaque (crime).

2) Est crime, tout objectif qui vise un intérêt relatif au : vol des informations à des buts de les exploiter ou de les vendre,
3) Appel à des astuces intelligentes aux actions de kidnappage et de demande de rançons.
4) Destruction des systèmes informatiques pour nuire le fonctionnement d'un Etat, d'une institution, d'une ou plusieurs entreprises.
5) Nuisance qui consiste à tester les capacités technologiques de malveillance, de dégradation, ou de détérioration de qualité de service d'un système réseautique informatique ou du réseau internet.
6) Pratique d'espionnage aux personnes non agréées ou non assermentées.
7) Usage du numérique pour des informations malveillantes, fausses, injustes, truffées de mensonges, ou d'informations tronquées diffusées aux réseaux sociaux en vu de ternir l'image de marque, ou par l'atteinte à la dignité d'autrui à travers des photos cinématiques muettes, sonores ou animées.

Titre 2.
De l'application de la loi pénale.
Chapitre 2
Dispositions préliminaires-Infractions,

Article 3 : Mode opératoire des cybernautes criminels

1) Les cybercriminalités identifiées comme hackers, arnaqueurs, ou pirates sont des individus qui opèrent par fishing ou hameçonnage dont l'objectif vise l'usurpation d'identité pour avoir accès aux données personnelles d'autrui.
2) Ils opèrent par Spamming (mails indésirables).
3) Les cybers attaques sont également ces bandits qui opèrent par intrusion des virus pour prendre frauduleusement le contrôle d'un système par des logiciels et/ou des applications malveillantes qui affectent ou détruisent le fonctionnement des systèmes informatiques.
4) Ils opèrent aussi par scanning, une opération de vol et d'escroquerie d'argent en ligne par le réseau internet
5) Ils opèrent également par la constitution des réseaux de kidnappage pour extorquer de l'agent ou obtenir de rançon.
6) D'autres opèrent par indécence aussi par provocation faisant usage aux comportements déviants aux bonnes mœurs en diffusant des images indécentes et immorales, émettant des propos injurieux, des discours de haine et d'humiliation entraînant la désolation, de l'indignation et des conflits sociaux.

Titre 3.
De l'application de la loi pénale
Chapitre 3
Dispositions préliminaires et préventions,

Article 4 : Mesures à apprendre pour combattre le fléau

1) Mise en place d'un cadre globale de régulation de surveillance des services du numérique et une plateforme de normalisation définissant les règles de lois universelles pour la sécurité de l'utilisation de l'internet et de l'encadrement du comportement des internautes en fixant des limites sur l'usage de la qualité d'informations et de la véracité authentique des sources du type de message diffusé dans les réseaux sociaux et dans les médias.
2) Le régulateur doit effectuer régulièrement les audits sécuritaires des systèmes informatiques afin d'évaluer le degré de vulnérabilité en veillant à quel point un système informatique présente des failles et des risques.
3) Former des experts en sécurité des systèmes informatiques pour effectuer la veille sécuritaire afin de répondre de façon proactive aux cybers attaques.
4) Vulgariser la certification identitaire en utilisant les procédés électroniques internationales pour garantir la confidentialité, la véracité, l'intégrité, l'authenticité et la non répudiation des données d'informations.
5) Informer, Eduquer, Conscientiser et Sensibiliser en orientant les populations sur la notion de morale de bonne conduite et les bonnes manières à mieux faire usage des outils modernes de technologies de l'information et de la communication à l'internet, à la radio et à la télévision. Ceci en montrant clairement les limites de leur liberté et la responsabilité des opérations qu'ils engagent et qu'ils devront assumer.

Titre 4.
De l'application de la loi pénale
Chapitre 4
Responsabilité pénale des personnes morales et physiques,

Article 5 : Peine et responsabilité

1) Est pénalement responsable, celui qui volontairement commet les actes constitutifs d'une infraction avec l'intention de nuire autrui ou a pour conséquence la réalisation de l'infraction ou à déstabiliser l'ordre de la nature sociale positive humaine, l'ordre du système fonctionnel de la bonne marche structurelle évolutive d'une entreprise publique ou privée.

Articles 6 : Personnes physiques ou morales pénalement responsables

1) Les individus mal intentionnés, les sociétés de fournisseur de réseau internet et de diffusion des informations en messages écrits ou images visuelles sonores et animées qui favorisent la publication des informations fausses et mensongères à caractère haineux pour nuire, avilir, ou susciter une indignation injustement à autrui , ou à diffuser des propos dilatoires pour créer un sentiment anti communautaire mettant en péril les notions de civisme, de citoyenneté, de bonnes mœurs et compromettant le vivre ensemble est pénalement responsable.

Article 7 : Conspiration cybernétique criminelle

1) Il ya conspiration par acte à l'exécution criminelle cybernétique lorsque la résolution de commettre une infraction inique ou sadique est concertée entre deux (2) ou plusieurs personnes qui peuvent être personnes physique ou personnes morales.

Article 8 : Coaction et de la complicité

1) Il ya coaction et complicité lorsque les deux (2) infractions sont liées aux objectifs visant les stratégies de l'usage des technologies de l'information et de la communication à des fins criminelles.

Article 9 : Coaction

1) Est Co acteur celui qui participe avec autrui un accord tacite par une entente de fait et avec consentement ou non à la commission d'une infraction du crime cybernétique.

Article 10 : Complice

1) Est complice d'une infraction, les cybernautes et/ou les utilisateurs des réseaux sociaux pour usage d'une infraction qualifiée de crime ou de délit : celui qui provoque, de quelque manière que ce soit la commission de l'infraction ou donne des instructions pour la commettre ;
2) Celui qui fait l'apogée et encourage les actes criminels, celui qui aide ou facilite la préparation ou la réalisation de l'infraction cybernétique criminelle par production, par émission, par diffusion ou par publication.
3) La tentative de complicité est considérée comme complicité. Sauf en cas de dénonciation. Le complice bénéficie des circonstances atténuantes et de protection de sa vie physique.

Titre 5.
De l'application de la loi pénale
Chapitre 5
Sanction et exécution des peines

Article 11 :
Est puni d'un emprisonnement de 5 à 25 ans et d'une amande de 50 000 à 500 000 euros ou une de ces deux peines, toute personne reconnue coupable de sabotage, de piratage, de vol qualifié avec des circonstances aggravantes aux systèmes informatiques d'entreprises privées ou publiques, d'avoir émis ou d'avoir propagé ou diffusé des informations nuisibles et mensongères, lorsque ces nouvelles fausses sont susceptibles de nuire à la dignité et à l'honorabilité aux autorités publiques, à autrui ou à la cohésion sociale, nationale et internationale.
En cas de réduction de la peine prévue à l'article 5, ci-dessus la peine de privation de liberté est celle de l'emprisonnement ferme.

Article 12 :
1) Est puni d'un emprisonnement de 10 à 30 ans et d'une amende de 35 000 à 75 000 euros ou de l'une de ces deux peines seulement celui qui diffuse ou qui relais les informations mensongères et propage les images photographiques, télématiques ou cinématiques muettes, ou sonores tronquées de l'intimité, de la dignité ou de l'honorabilité d'autrui.
2) Une entreprise fournisseur de réseaux sociaux de communication ou de télématique audiovisuelle impliquée à cette diffusion est reconnue complice au titre des articles 5, 6, 7, 8, 9 et 10.

L'entreprise y associé subit un arrêt provisoire de ses services d'une fermeture de 3 à 6 mois et d'une amande de 500 000 à 5000 000 euros.

Article 13 :
Sont punis d'un emprisonnement de 10 à 30 ans et d'une amende de 35 000 à 75 000 euros ou de l'une de ces deux peines seulement, tout membre d'une association et/ou regroupement de malfaiteurs ou complice constitués en entreprise de pirates de l'air, maritime et/ou de kidnappeurs et de rapt pour besoin de rançonnage faisant usage des outils de technologie moderne de l'information et de la communication pour des fins criminelles.

Article 13 :
Est puni d'un emprisonnement de 3 à 5 ans et d'une amende de 5 000 à 25 000 euros ou de l'une de ces deux peines seulement, toute personne qui expose, publie ou relais dans les réseaux sociaux ou dans les entreprises médiatiques la nudité de l'intimité d'autrui ainsi considéré de violence faite à la dignité et à l'honorabilité humaine.

Emmanuel So'o Ateba
Directeur Administratif Responsable de la Plateforme relais
Chargé des projets et de missions de coopération de solidarité
Bureau de la Solidarité internationale
ACEH-Les Compagnons Solidaires.

http://aceh-lescompagnonssolidaires.e-monsite.com
https://www.facebook.com/ACEH-Lescompagnonssolidaires-ActionTerredAfriaue/