**DRAFT DE LA CONVENTION INTERNATIONALE GLOBALE SUR LA LUTTE CONTRE L'UTILISATION DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION A DES FINS CRIMINELLES**

## PREAMBULE (Objectifs et champ d'application)

## CHAP I. DES DEFINITIONS

Au sens de la présente Convention, on entend par :

**Accès illicite** : accès intentionnel, sans en avoir le droit, à l'ensemble ou à une partie d'un réseau de communication électronique, d'un système d'information ou d'un équipement terminal.

**Chiffrement** : toute technique consistant à transformer les données numériques en un format inintelligible en employant des moyens de cryptologie.

**Cryptologie** : science relative à la protection et à la sécurité des informations.

**Cybercriminalité** : tout fait illégal commis au moyen d'un système ou d'un réseau informatique ou de tout autre réseau physique connexe ou en relation avec un système d'information.

**Cyberespace** : ensemble de données numérisées constituant un univers d'informations et un milieu de communication lié à l'interconnexion mondiale d'équipement de traitements automatisé de données numériques.

**Cyber-sécurité** : ensemble de mesures de prévention, de protection et de dissuasion d'ordre technique, organisationnel, juridique, financier, humain, procédural et autres actions permettant d'atteindre les objectifs.

**Communication électronique** : toute émission, transmission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de vidéos par voie électromagnétique, optique ou par tout autre moyen.

**Données à caractère personnel** : toute information de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique.

**Données informatiques** : désigne toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction.

**Electromagnétique** : résultat de la vibration couplée d'un champ électrique et d'un champ magnétique variable dans le temps.

**Fournisseurs de services :** personne physique ou morale qui fournit un ou plusieurs **services** aux utilisateurs d'un système de télécommunication.

**Information** : tout élément de connaissance susceptible d'être représenté à l'aide de conventions pour être utilisé, conservé, traité ou communiqué. L'information peut être exprimée sous forme écrite, visuelle, sonore, numérique, ou autre.

**Infrastructure critique** : infrastructure qui est essentielle aux services vitaux pour la sureté publique, la stabilité économique, la sécurité nationale, la stabilité internationale et pour la pérennité et la restauration du cyberespace critique.

Les infrastructures critiques de l'Etat sont constituées par les services de santé publique, de sécurité intérieure et extérieure, de défense, des finances et des transports connectées aux réseaux internet.

**Interception illégale** : accès sans en avoir le droit ou l'autorisation, aux données d'un réseau de communications électroniques, d'un système d'information ou d'un équipement terminal.

**Gateway internationale** : nom générique d'un dispositif permettant de relier deux réseaux informatiques de types différents par exemple un réseau local et le réseau internet.

**Moyen de paiement électronique** : moyen permettant à son titulaire d'effectuer des opérations de paiement électroniques en ligne.

**Phishing/fishing** : C'est une forme d'escroquerie par mail qui consiste à prendre l'identité d'une entreprise connue et reconnue sur un e-mail pour inciter les destinataires à changer ou mettre à jour leurs coordonnées bancaires sur des pages internet imitant celles de l'entreprise dont l'image a été utilisée pour l'escroquerie.

**Pornographie infantile** : Toute représentation visuelle d'un comportement sexuellement explicite y compris toute photographie, film, vidéo, image que ce soit fabriquée ou produite par voie électronique, mécanique ou par autres moyens où :

1° la production de telles représentations visuelles implique un mineur ;
2° les représentations visuelles sont une image numérique, une image d'un ordinateur ou une image générée par un ordinateur où un mineur est engagé dans un comportement sexuellement explicite ou lorsque des images de leurs organes sexuels sont produites ou utilisées à des fins principalement sexuelles et exploitées à l'insu de l'enfant ou non ;
3° la représentation visuelle a été créée, adaptée ou modifiée pour qu'un mineur engage dans un comportement sexuellement explicite.

**Prestataires de services** : les opérateurs mobiles, les fournisseurs d'accès internet ainsi que les opérateurs d'infrastructures

**Programme informatique** : Ensemble d'instructions exécutées par l'ordinateur pour obtenir les résultats escomptes.

**Raciste et xénophobe en matière des TIC**: tout matériel 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 ou de l'origine nationale ou ethnique ou de la religion.

**Spamming** : envoi généralement massif et non ciblé, de messages commerciaux par e-mail avec l'intention de voler, à des individus n'ayant pas donnés leur autorisation à l'émetteur pour la réception de tels messages.

**Système informatique** : Désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données.

**TIC** : Technologie de l'Information et de la Communication.

## CHAPITRE II. DES INFRACTIONS CONTRE LA CONFIDENTIALITE, L'INTEGRITE ET LA DISPONIBILITE DES DONNEES ET DES SYSTEMES INFORMATIQUES

### Section 1. De l'atteinte à la confidentialité des systèmes informatiques

### Section 2. De l'accès illégal

Les Etats partis à la présente convention doivent ériger en infraction pénale, conformément à la loi interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique.

### Section 3. De l'atteinte à l'intégrité du système informatique

Les Etats partis à la présente convention doivent ériger en infraction pénale, conformément a la loi interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.

### Section 4. De l'atteinte à l'intégrité des données

Les Etats partis à la présente convention, doivent ériger en infraction pénale, sans préjudice a la loi interne, l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération et la suppression de données informatiques

## Section 5. De la fabrication, vente, achat, utilisation, importation, distribution ou possession illégale d'un système informatique et de l'incitation au suicide

Les Etats partis à la présente convention doivent ériger en infraction pénale sans préjudice à loi interne, la fabrication, la vente, l'achat, l'utilisation, l'importation, la distribution ou la possession d'un ordinateur ou d'un système informatique, ou rendre disponible les données, les programmes ou le système informatique avec l'intention de les utiliser ou les met à la disposition d'autrui dans le but de commettre des infractions.

## Section 6. De la fraude informatique

Les Etats partis à la présente convention doivent ériger en infraction pénale sans préjudice à loi interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui par: a. l'introduction, l'altération, l'effacement ou la suppression de données informatiques, b. toute forme d'atteinte au fonctionnement d'un système informatique, dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui.

### §1. De l'escroquerie dans les systèmes informatiques

Les Etats partis à la présente convention doivent ériger en infraction pénale sans préjudice à loi interne, le fait d'user de manœuvre frauduleuse, et au moyen de communication électronique, pour se faire remettre ou délivrer, tenter de se faire remettre ou délivrer des fonds, des meubles, des obligations, des dispositions, des billets, des promesses, des quittances, des décharges, tout ou une partie de la fortune d'autrui.

### §2. De l'usurpation d'identité numérique

Les Etats partis à la présente convention doivent ériger en infraction pénale sans préjudice à loi interne, le fait d'usurper l'identité numérique d'un tiers ou de faire usage d'une ou de plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou de porter atteinte à son honneur, à sa vie privée, à son patrimoine ou à celui d'un tiers pour tirer profit ou pour induire en erreur d'autres personnes.

### §3. Du Phishing

Les Etats partis à la présente convention doivent ériger en infraction pénale sans préjudice à loi interne, le fait d'utiliser un site web ou d'envoyer un message électronique à l'aide d'un système informatique avec l'intention d'obtenir des informations confidentielles du visiteur du site ou du destinataire du message pour s'en servir à des fins criminelles.

**§4. De l'abus de confiance portant sur les données informatiques**

Les Etats partis à la présente convention doivent ériger en infraction pénale sans préjudice à loi interne, le fait de détourner ou de dissiper des données informatiques remis à titre quelconque, à charge de les restituer ou d'en faire un usage déterminé.

**§5. Du recel des données informatiques**

Les Etats partis à la présente convention doivent ériger en infraction pénale sans préjudice à loi interne, détient sciemment, à un titre quelconque, des données informatiques obtenues à l'aide d'une infraction.

**§ 6. De l'extorsion des données informatiques**

Les Etats partis à la présente convention doivent ériger en infraction pénale sans préjudice à loi interne, le fait de tenter de se faire remettre par force, violence ou contrainte des données informatiques.

**§7. Du chantage et de la publication des rumeurs**

Les Etats partis à la présente convention doivent ériger en infraction pénale sans préjudice à loi interne, le fait de menacer par des écrits ou verbalement, de révélation ou d'imputation diffamatoire, extorquer ou tenter d'extorquer des données informatiques.

**§ 8. Du spamming**

Les Etats partis à la présente convention doivent ériger en infraction pénale sans préjudice à loi interne, les faits suivants :

1° envoie des messages non sollicités à plusieurs reprises ou à un grand nombre de personnes en utilisant un ordinateur ou un system informatique ;

2° après avoir reçu un message, utilise un ordinateur ou un système informatique pour retransmettre ce message à plusieurs personnes ou le retransmettre plusieurs fois à une personne qui n'en a pas besoin.

**Section 7. Des infractions se rapportant au contenu**

**§1. Infractions se rapportant à la pornographie enfantine**

Les Etats partis à la présente convention doivent ériger en infraction pénale sans préjudice à loi interne, les comportements suivants lorsqu'ils sont commis intentionnellement et sans droit: la production de pornographie enfantine en vue de sa diffusion par le biais d'un système informatique; l'offre ou la mise à disposition de pornographie enfantine par le biais d'un système ;

**Section 8. Des écrits et images de nature raciste ou xénophobe par le biais d'un système informatique**

Les Etats partis à la présente convention doivent ériger en infraction pénale sans préjudice à la loi Interne, le fait de créer, télécharger, diffuser ou mettre à la disposition sous quelque forme que ce soit des écrits, messages, photos, dessins, vidéos ou toute autre représentation d'idées ou de théories, de nature raciste ou xénophobe, par le biais d'un système informatique.

**Section 09. De l'injure commise par le biais d'un système informatique**

Les Etats partis à la présente convention doivent ériger en infraction pénale sans préjudice à
La loi Interne, le fait d'injurier 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 ou la religion dans la mesure où cette appartenance sert de prétexte à l'un ou l'autre de ces éléments, ou un groupe de personnes qui se distingue par l'une de ces caractéristiques,

**Section 10. Des infractions liées au terrorisme, à la fabrication des armes, au trafic des personnes ou de stupéfiants commises à l'aide d'un ordinateur ou d'un système informatique**

**§1. De la création ou de la publication d'un site pour les groupes terroristes**

Les Etats partis à la présente convention doivent ériger en infraction pénale sans préjudice à
la loi Interne, le fait de :

1° d'établir, de publier ou d'utiliser un site d'un groupe terroriste à l'aide d'internet, d'un ordinateur ou d'un système informatique afin de faciliter la communication par son leadership ou ses membres,
2° de mobiliser des fonds ou diffuse ses idées ou connaissances sur la façon dont il mène ses opérations de nature terroriste.

**§2. De la diffusion de procédé ou moyen de destruction**

Les Etats partis à la présente convention doivent ériger en infraction pénale sans préjudice à loi interne, le fait de diffuser ou mettre à disposition d'autrui par le biais d'un système informatique, sauf à destination des personnes autorisées, un mode d'emploi ou des procédés permettant la fabrication des armes à feu, de leurs pièces, éléments et munitions de nature à porter atteinte à la vie humaine, aux biens ou à l'environnement.

### §3. De la création ou publication d'un site dans le but de la traite des êtres humains

Les Etats partis à la présente convention doivent ériger en infraction pénale sans préjudice à loi interne, établit ou publie un site sur un réseau d'information, un matériel informatique ou un système informatique à des fins de traite des personnes ou qui facilite une telle transaction.

### §4. De la création ou publication d'un site dans le but de trafic ou de distribution de drogues ou de stupéfiants

Les Etats partis à la présente convention doivent ériger en infraction pénale sans préjudice à loi interne, le fait de créer un site ou publier, sur un réseau d'information, un matériel informatique ou système informatique pour trafic ou distribution de drogues ou de stupéfiants ou facilitant une telle transaction.

### Section 11. De l'association de malfaiteurs informatiques

Les Etats partis à la présente convention doivent ériger en infraction pénale sans préjudice à loi interne, le fait de participer intentionnellement à une association formée ou à une entente établie en vue de préparer ou de commettre une ou plusieurs infractions

### Section 12 : Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

Les Etats partis à la présente convention doivent ériger en infraction pénale sans préjudice à loi interne, les atteintes à la propriété intellectuelle.

## CHAPITRE III DE LA RESPONSABILITE DES PERSONNES MORALES

Les Etats partis à la présente convention doivent prendre les dispositions nécessaires pour faire en sorte que les personnes morales puissent être tenues pour responsables des infractions établies par la présente convention.

Adopter les mesures nécessaires pour s'assurer qu'une personne morale puisse être tenue pour responsable en l'absence de surveillance ou de contrôle de la part d'une personne physique travaillant à son sein. La responsabilité de la personne morale pouvant être pénale, civile ou administrative.

### Section 13 : des obligations des fournisseurs de services et opérateurs de réseaux

Les données relatives aux abonnés doivent être conservées par les fournisseurs de services.

Ces derniers ont l'obligation de conserver et de protéger l'intégrité desdites données pendant une durée de dix ans minimum.

**§1.** Les fournisseurs de services de communication électronique ont l'obligation de :

1° informer leurs clients des tendances de la cybercriminalité qui les affectent ou qui peuvent les affecter ;
2° établir une manière procédurale de signaler la cybercriminalité à leurs clients ;
3° informer leurs clients des mesures qu'ils peuvent prendre pour se protéger contre la cybercriminalité ;
4° révéler les abus à la victime concernée et aux organes chargés de la répression de la cybercriminalité.

**§.2** Tout fournisseur de service qui connait ou prend connaissance que son ordinateur ou son système informatique ou son réseau de communication électronique est utilisé pour commettre une infraction prévue par la présente loi a l'obligation de :

1° signaler immédiatement l'incident aux services chargés de l'investigation et de l'instruction criminelles ;
2° conserver toute information susceptible d'aider à enquêter sur l'infraction comme l'origine, la destination, l'itinéraire, l'heure, la date, la dimension, la durée de la communication et le type de services sous-jacents.

**§3.** Tout fournisseur de service qui prend connaissance ou qui a été mis au courant par les organes habilités, des informations ou activités illégales a l'obligation de :

1° empêcher l'accès à ces informations ;
2° suspendre ou mettre fin aux services du client ayant lancé des informations ou entrepris des activités illégales ;
3° donner des informations nécessaires aux organes ayant l'investigation ou la poursuite judiciaire dans leurs attributions.

**§4.** Les opérateurs des réseaux de communications électroniques et les fournisseurs de services de communications électroniques ont l'obligation de garantir la sécurité des services offerts. Ils doivent mettre en place les procédés et moyens techniques permettant de lutter contre la fraude téléphonique internationale.

## CHAPITRE IV : DE LA COOPERAION INTERNATIONALE

**§1.** Les États Parties s'engagent à favoriser les échanges d'informations ainsi que le partage efficient des données sur une base bilatérale et multilatérale, privilégier des réunions techniques régionales et internationales dans le but de faire face à l'évolution sans doute exponentielle de la cybercriminalité dans le monde.

**§2.** Les États Parties s'engagent à encourager la mise en place des institutions qui échangent des informations sur les cybermenaces et sur l'évaluation de la vulnérabilité telles que les équipes de réaction d'urgence en informatique (CERT : Computer Emergency Response Teams) ou les équipes de réaction aux incidents de sécurité informatique (CSIRTS : Computer Security Incident Response Teams).

**§3.** Les États Parties s'engagent à se prévaloir de moyens existants pour la coopération internationale aux fins de répondre aux cybermenaces, à améliorer la cybersécurité et à stimuler le dialogue entre les parties prenantes. Ces moyens pourraient être internationaux, intergouvernementaux ou régionaux, ou basés sur des partenariats privés et publics.

**§4.** Les Etats Parties s'engagent à développer les mécanismes de renforcement des capacités opérationnelles et professionnelles (en équipements et formations) des centres ou services nationaux dans le but de prévenir, mener des enquêtes et poursuivre les auteurs des crimes liés à l'usage des technologies de l'information et des télécommunications.

## CHAPITRE V : DES DSIPOSITIONS FINALES

### §1. Des mécanismes de suivi de la mise en application de la présente convention

**§2. Du règlement des différends :** Tout différend qui émerge dans le cadre de l'interprétation ou de la mise en application des dispositions de la présente Convention entre les Etats Parties et de ses mesures d'exécution sera réglé à l'amiable ou par voie diplomatique, ou à défaut par des juridictions internationales compétentes.

**§3. De la signature, de l'adoption et de la ratification :** La présente Convention est ouverte à tous les États membres, pour signature, ratification et adhésion, conformément à leurs procédures constitutionnelles respectives.

**§4. De l'entrée en vigueur de la présente Convention :** La présente Convention entre en vigueur pour une durée indéterminée dès son adoption par l'Assemblée Générale des Nations Unies et sa ratification par les Etats Parties.