RÉPUBLIQUE DU SÉNÉGAL

Un Peuple – Un But – Une Foi

2e Session du Comité ad hoc chargé d'élaborer une Convention des Nations Unies sur la lutte contre l'utilisation des technologies de l'information et de la communication à des fins criminelles

Vienne, du 30 mai au 10 juin 2022

****

Réponses du Sénégal aux questions directrices de la Présidente du Comité

****

I. INCRIMINATIONS.

A. PREMIER GROUPE DE QUESTIONS.

Réponse à la question 1.

L'intention frauduleuse doit être prise en compte pour caractériser les infractions d'atteintes à la confidentialité, a la disponibilité et à l'intégrité des données et systèmes informatiques car nous considérons que l'auteur doit avoir la claire conscience de commettre l'acte interdit. Cela permet de garantir la sécurité juridique et réaffirmer le principe de la responsabilité pénale.

Les termes, sans droit, sans autorisation ou frauduleusement peuvent être employés, en fonction des comportement et selon les législations nationales. Ces garanties légales permettent de protéger les professionnels du net, les chercheurs et les fonctionnaires étatiques chargés de lutter contre ces formes de criminalité.

La tentative et la complicité de ces infractions doivent être prévues dans la convention afin d'assurer une protection pénale optimale des données et des systèmes informatiques.

Réponse à la question 2.

L'existence d'un préjudice matériel ou économique pourrait ne pas être exigé, mais l'accent devrait plutôt être mis sur le comportement fautif ou malveillant de l'auteur de l'infraction et sur son intention de porter atteinte à la sécurité, la tranquillité et l'environnement du cyberespace.

Réponse à la question 3.

La violation d'une mesure de sécurité pourrait être retenue comme condition pour établir certaines infractions, surtout lorsqu'elle consiste en un comportement de nature à contourner délibérément une telle mesure de sécurité, avec l'intention d'enfreindre la réglementation liée au cyberespace.

Réponse à la question 4.

La délégation sénégalaise préfère d'abord attendre de prendre connaissance aux dispositions qui ont été proposées relativement à « l'obstruction d'un ordinateur, programme ou données », « Attaque sur une conception de site », afin d'émettre un avis éclairé sur cette question.

Réponse à la question 5.

La convention devrait traiter la question de l'accès non autorisé ou l'interférence avec une information critique d'infrastructure de la manière la plus dissuasive et répressive possible.

En ce sens, les infrastructures nationales critiques comme cible des agissements cybercriminels peuvent être pris en compte comme circonstances aggravantes dans la détermination de la sanction pénale.

B. DEUXIÈME GROUPE DE QUESTIONS

Réponse à la question 1.

Le délit de fraude, commis en tout ou partie en ligne, ne nous semble pas suffisant pour couvrir les autres comportements tels que le vol, l'escroquerie, les délits financiers, et les infractions liées aux outils de paiement électronique. Ces comportements, bien qu'ayant un objet infractionnel en commun, en l'objet la propriété, n'ont pas nécessairement les mêmes éléments caractéristiques.

Dès lors, ils pourraient être traités différemment si on entendait les prendre tous en charge, à travers la future convention.

Réponse à la question 2.

La falsification informatique est le pendant de la falsification des documents sur papier. Elle vise à combler les lacunes du droit pénal se rapportant à la falsification classique, laquelle ne s'applique pas aux données informatiques enregistrées sur un support électronique.

La manipulation de ces données ayant une certaine force probante peut induire en erreur un tiers. Sa constitution doit supposer la caractérisation d'un acte matériel de faux notamment l'altération de la vérité et l'emploi de moyens frauduleux spécifiques, à savoir résulter de l'effacement, de la suppression ou de l'introduction frauduleuse de données informatisées stockées, traitées ou transmises par un système informatique.

Réponse à la question 3.

L'usage en connaissance de cause de données informatiques falsifiées pourrait être inclus dans les formes de falsification informatique.

Réponse à la question 4.

L'usurpation d'identité numérique pourrait être incriminée spécifiquement dans la future convention, en ce sens qu'elle pourrait aussi procéder d'une motivation autre que financière. C'est le cas par exemple lorsqu'un délinquant usurpe l'identité d'une personne pour brouiller les pistes afin d'éviter d'être identifié facilement par les autorités de poursuite.

Réponse à la question 5.

Les atteintes au droit d'auteurs et droits voisins nous semble avoir été suffisamment pris en compte par d'autres instruments internationaux et régionaux, et les inclure dans la future convention risquerait d'alourdir le texte, et entraînerait des divergences conceptuelles dans la prise des infractions concernées.

C. TROISIÈME GROUPE DE QUESTIONS

Réponse à la question 1.

Les infractions liées à l'abus sexuel d'enfants en ligne pourrait être définies de manière suffisamment large pour garantir une meilleure protection de cette couche vulnérable de la société.

Le choix de la terminologie doit s'appuyer sur des comportements et moyens techniques utilisés par les délinquants pour cibler les enfants.

Les définitions contenues dans la Convention de l'Union africaine et du Conseil de l'Europe sur la cybercriminalité nous semblent assez pertinentes pour être reproduites dans la rédaction de la future Convention.

Réponse à la question 2.

La future Convention pour inclure dans les incriminations relatives à la pornographie enfantine, les comportements tels que le partage et la possession en connaissance de cause d'une image ou d'une représentation présentant un caractère de pornographie enfantine dans un système informatique ou dans un moyen quelconque de stockage de données informatiques.

Plus concrètement, il s'agirait d'incriminer non seulement le risque d'exploitation sexuelle des mineures, notamment par la création d'incriminations spécifiques à la pornographie enfantine mais également le risque d'exposition des mineurs à des contenus illicites à savoir la criminalisation de la facilitation de l'accès des mineurs à des images présentant un caractère de pornographie enfantine et celle de l'accès avec connaissance à la pornographie enfantine.

L'obligation d'incriminer ces actes peut, toutefois, être assortie des formules telles que conformément aux principes juridiques ou à la législation nationale des États parties ou sans préjudice du droit interne des États parties, afin de protéger certains types d'exploitation de ces images, liées à des activités scientifiques ou professionnelles.

Réponse à la question 3.

La plupart des conventions régionales ou internationales, notamment la Charte Africaine des Droits et du bien-être de l'enfant de 1990 et la convention des Nations Unies sur les droits de l'enfant, considèrent comme mineur toute personne âgée de moins de 18 ans. Nous pensons que la future convention doit aller dans le même sens afin d'éviter une diversité du régime juridique de la notion d'enfant.

Nous pensons que la sexe torsion doit être incriminée dans la convention afin de protéger les enfants contre ces types d'abus sexuel.

Les abus sexuels en ligne, notamment les formes de chantage, sont de plus en plus fréquents, et l'absence d'harmonisation de législations nationales rendent difficile l'utilisation des mécanismes de coopération pour les réprimer, d'autant que pour la plupart des pays comme ceux en développement, la collaboration des fournisseurs d'accès et de services, souvent situés hors de leurs frontières est indispensable, pour permettre l'efficacité des poursuites et de la répression.

Réponse à la question 4.

L'inclusion des dispositions tendant à incriminer l'incitation ou la contrainte d'un mineur au suicide ou à la commission d'une infraction, dans la future convention, pourrait être justifiée par le besoin de protection de l'intérêt supérieur de l'enfant.

Cela pourrait permettre de surmonter l'obstacle de la non-incrimination de la complicité du suicide dans la plupart des législation, mais aussi protéger les mineurs contre certains comportements dont ils pourraient être victimes, et qui ne soient pas forcément de nature sexuelle, mais qui pourrait les pousser aux suicides ou les mettre dans un état de dépression critique, ou en danger.

Réponse à la question 5.

La liberté d'expression doit être garantie, mais cette liberté ne doit pas être le prétexte pour un individu de s'adonner à des actes d'injures, de menace, de chantage ou violation de la vie privée d'autrui. La non-incrimination par certains pays de la diffusion de messages offensant par le biais des TIC, a conduit à la multiplication de ces types de comportements dans le cyberespace, et les personnes qui s'adonnent à cela choisissent de s'établir dans les États où ils se sentiraient impunis.

D. QUATRIÈME GROUPE DE QUESTIONS.

Réponse à la question 1.

La future convention pourrait contenir des dispositions conférant le caractère d'infraction pénale, lorsque l'acte aura été commis intentionnellement, au fait par toute personne de créer, télécharger, diffuser ou mettre à dispositions, 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.

Les questions liées à la distribution de stupéfiants, de substances psychotropes, de trafic d'armes, ainsi qu'à la distribution illégale de médicaments et de produits

médicaux contrefaits, et à la traite des personnes pourraient être laissées aux instruments internationaux ayant déjà traité ces domaines de criminalité.

Réponse à la question 2.

La future convention pourrait inclure une disposition relative à l'obligation pour tout État membre de juger toute personne se trouvant sur son territoire, ayant commis des faits qualifiés d'infractions cybercriminelles, ou de l'extrader.

Réponse à la question 5.

La définition des crimes de droit international nous semble avoir été pertinemment pris en charge par le Statut de Rome et les autres conventions y relatives, et il n'est pas nécessaire de prévoir des dispositions les concernant dans la future convention, au risque de créer des régimes différents et des difficultés d'interprétation.

E. CINQUIÈME GROUPE DE QUESTIONS.

Réponse à la question 1.

Le Sénégal pense que l'inclusion d'une incrimination sur l'entrave de la justice et du blanchiment du produit des crimes ne serait pas nécessaire, dans la mesure où ces incriminations ont déjà prises en charge, et de manière pertinente, par d'autres instruments internationaux, notamment la Convention des Nations Unies contre la criminalité transnationale organisée. Une nouvelle prise en charge pourrait contraster d'avec les dispositions préexistantes.

En revanche, une référence à la convention susvisée afin de réaffirmer l'inclusion des infractions cybercriminelles dans la catégorie des infractions sous-jacentes au blanchiment de capitaux pourrait être envisagée.

Réponse à la question 2.

La future convention pourrait traiter les aspects liés à la participation, la tentative, ainsi qu'à l'aide et à l'assistance en vue de la commission d'une infraction, dans des dispositions générales, en se gardant de spécifier les comportements, qui pourraient en découler, et en laissant aux États parties le soin d'apprécier des modalités de leur incorporation dans leur droit interne, surtout que la plupart des systèmes juridiques disposent déjà de dispositions relatives à ces questions.

Réponse à la question 3.

La responsabilité pénale dans le cyberespace doit être étendue aux personnes morales. C'est la position que le Sénégal a adopté en intégrant dans son droit pénal interne une disposition qui prévoit une telle responsabilité. C'est également cette même position que notre pays a pris dans sa contribution au projet de convention. Nous pensons que la responsabilité des personnes morales doit être établie par rapport aux infractions prévues par la convention lorsqu'elles ont été commises pour leur compte et par leurs représentants. Cette responsabilité peut être pénale, civile ou administrative et ne doit pas exclure celle des personnes physiques auteurs ou complices des mêmes faits. La convention doit enfin inviter les États parties à veiller à ce que les personnes tenues responsables fassent l'objet de sanctions efficaces,

proportionnées et dissuasives pénales et non pénales, y compris des sanctions pécuniaires.

Réponse à la question 4.

La formulation de la responsabilité des personnes morales au sens de l'article 10 de l'UNTOC nous semble pertinente pour prendre en charge, les infractions cybercriminelles impliquant de telles personnelles.

La question de la négligence pourrait toutefois être considérée comme un comportement punissable dès lors qu'aucune mesure minimale de sécurité n'aurait être prise en charge par la personne morale concernée.

Réponse à la question 5.

Nous estimons que la convention doit contenir une dispositions générale sur les circonstances aggravantes ou atténuantes en laissant aux États membres le soin de déterminer au niveau interne les conditions de leur application.

II. DISPOSITIONS GÉNÉRALES

Réponse à la question 1.

Le choix devrait consister à adopter une convention qui a un objet précis et limité mais fort afin d'appréhender les comportements actuels et futurs, spécifiques ou en rapport avec l'utilisation des TIC.

Réponse à la question 2.

La nécessité de prendre en charge l'évolution rapide des technologies de l'information et de la communication ne doit pas nous faire perdre de vue des principes sacro sains comme l'interprétation stricte du droit pénal de fond, ainsi que les exigences de certitude, d'accessibilité et de prévisibilité de ladite matière.

La prochaine convention devrait autant que faire se peut couvrir la définition des concepts les plus complexes liés au cyberespace, et être le moins équivoques possibles.

La prise en charge de comportements illicites futurs dans le cyberespace, pourrait amener à s'appuyer sur d'éventuels protocoles additionnels.

Pour autant, il serait nécessaire de recourir à des termes technologiquement neutres, afin de tenir compte de l'évolution rapide des TIC, pour éviter que la convention ne soit vite dépassée.

Réponse à la question 3.

Un chapitre sur les dispositions dans la même structuration que l'UNTOC et l'UNCAC nous parait important pour mieux asseoir la pertinence de la prochaine convention,

et tenir compte de la postérité, en ce sens qu'un tel chapitre permettra dans le futur de mieux percevoir ses objectifs, et de garantir la pérennité de son application.

Réponse à la question 4.

La déclaration d'intention devra mettre l'accent sur la protection de la souveraineté des États ainsi qu'une sur la réelle volonté de lutter contre la cybercriminalité qui constitue une menace pour les États, les organisations internationales, les entreprises et les personnes physiques.

Réponse à la question 5.

La question de la protection des droits de l'homme pourrait être prise en charge, dans le sens d'un équilibre entre le besoin d'exercice des libertés fondamentales et les exigences de protection des personnes et de leurs biens.

Réponse à la question 6.

La preuve électronique doit être élargie à la poursuite et à la répression des infractions classiques, en ce sens que les nouvelles techniques d'investigations, notamment celles s'appuyant sur les technologies de l'information et de la communication ont libre court dans beaucoup de pays, et permettent généralement de rechercher plus efficacement des auteurs d'infractions transnationales. Elle constitue également un outil performant de coopération pénale internationale.

Réponse à la question 7.

La future convention doit inclure des dispositions relatives à la saisie et à la confiscation des instruments et produits liés aux infractions cybercriminelles, en ce sens que la saisie constitue une mesure pertinente dans la procédure pénale, et la confiscation lorsqu'elle n'est pas prévue, comme peine principale ou complémentaire, serait difficilement applicable, d'où la nécessité de les prendre en charge.

Réponse à la question 8.

Le Sénégal répond par l'affirmative, mais la réitération des dispositions des articles 4 de l'UNTOC et de l'UNCAC, ne serait pas de trop pour réaffirmer ce principe de la souveraineté des États.

Réponse à la question 9.

Le Sénégal propose la reprise des termes définies dans les conventions liées à la cybercriminalité déjà existants, en y ajoutant ceux qui ne sont pas encore pris en charge, notamment :

- Les données relatives au contenu
- Les données de trafic
- Les données de l'abonné

Réponse à la question 10.

La définition des termes pourrait être abordée après la négociation des articles de fond de la convention, afin d'avoir la certitude de ne pas omettre des termes essentiels.

Réponse à la question 11.

L'accent doit être mis sur la définition des « systèmes informatiques », qui est plus large, et qui a d'ailleurs pris en charge l'expression « dispositifs TIC ».

Réponse à la question 12.

La protection des femmes et des filles devrait être suffisamment prise en charge, par la future convention.

III. MESURES PROCEDURALES

A- PREMIER GROUPE DE QUESTIONS

Réponse à la question 1.

La question de la compétence devrait faire l'objet d'un chapitre autonome à défaut d'être intégrée dans les dispositions générales, en ce sens qu'elle fédère des aspects de droit pénal de fond (la loi applicable) et de procédure (juridiction compétente). Elle constitue plus un principe processuel qu'une mesure procédurale.

Réponse à la question 2.

La base d'établissement de la compétence pourrait se limiter à l'individu, comme cible, objet ou auteur de l'infraction. L'application de la compétence devrait découler du lieu de commission de l'infraction, la résidence de l'auteur ou de la victime, la résidence des coauteurs ou complices, et de tous lieux où l'infraction aura eu des effets.

Réponse à la question 3.

Le Sénégal appuie l'application des mesures procédurales à toute infraction, dont l'utilisation de la preuve numérique pourrait faciliter la répression. L'utilisation des mesures procédurales classiques a montré ses limites quant à la recherche des auteurs d'infractions ordinaires.

Réponse à la question 5.

L'utilisation des mesures procédurales intrusives devrait-être soumise à l'autorisation et au contrôle d'une autorité judiciaire, ou de toute autorité compétente conformément aux législations nationales. La violation des conditions d'utilisation prévues par la prochaine convention devrait être assorties de droit de recours, et d'éventuelle annulation des procédures**.**

B. DEUXIÈME GROUPE DE QUESTIONS

Réponse à la question 1.

La Convention devrait conférer aux autorités d'enquête et de poursuite les pouvoirs nécessaires à la prévention et la répression des infractions visées par la prochaine convention, dans la limite de l'exercice des droits fondamentaux, et les garanties d'un procès équitable.

Réponse à la question 4.

Les délais relatifs à la conservation des données, dans l'attente d'une demande par les autorités compétentes pour sa divulgation, devrait être le plus court possible, afin d'empêcher les retards abusifs, et les atteintes à la vie privée**.**

Réponse à la question 7.

Les perquisitions et saisies ainsi que l'interception de données devraient non seulement s'opérer en présence de commission d'une infraction liées aux TIC, mais aussi de recherche de preuve d'une infraction dont l'établissement nécessite la preuve électronique, cela est d'ailleurs prévus par certaines conventions internationales, notamment celle de Palerme, ainsi que des conventions régionales, dont la Directive de la CEDEAO relative à la lutte contre le blanchiment de capitaux et le financement du terrorisme.

Réponse à la question 8.

La Convention peut bien contenir les déclarations ou réserves concernant des dispositions procédurales afin de permettre une large ratification. Cependant, nous souhaitons que ces réserves ne puissent pas porter sur des garanties essentielles prévues par la convention.

C. TROISIÈME GROUPE DE QUESTIONS :

Réponse à la question 1.

À défaut de s'en limiter

Réponse à la question 3.

Le régime de la protection des victimes et témoins bien que prévue par la Convention de Palerme, et d'autres instruments internationaux, pourrait être réaffirmé dans la future convention sur la cybercriminalité. Il faudrait juste éviter de créer un régime, qui pourrait entraîner des divergences dans la prise en charge de cette question.

D. QUATRIÈME GROUPE DE QUESTIONS :

Réponse à la question 1.

La collecte et la recevabilité de la preuve électronique doivent être strictement encadrées, afin de garantir leur légalité, leur loyauté et leur intégrité.

Réponse à la question 2.

La convention devrait contenir des dispositions spécifiques aux techniques d'enquêtes spéciales, en ce sens que ces mesures et procédés sont de nature très intrusive, qu'ils méritent un traitement rigoureusement encadré.

Réponse à la question 4.

La Convention devrait spécialement traiter des mesures de coopération avec les autorités chargées de l'application de la loi, en restant bien évidemment dans la logique déjà tracée par l'UNTOC et les autres instruments internationaux pertinents.