Lettre ouverte à l'Assemblée générale de l'ONU: La proposition de convention internationale relative à la cybercriminalité menace les droits humains en ligne

Vos Excellences,

La coopération internationale est indispensable face au défi majeur que représente la lutte contre la cybercriminalité. Cependant, l'approche proposée dans le projet de résolution « Lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles » (A/C.3/74/L.11/Rev.1) à la Troisième Commission de l'Assemblée générale de l'ONU (AGONU) présente de graves lacunes et risque de restreindre l'utilisation de l'internet en faveur des droits humains et du développement social et économique. Les organisations soussignées exhortent votre délégation à voter contre un tel projet de résolution.

Cette résolution propose de « créer un comité d'experts intergouvernemental spécial à composition non limitée, représentatif de l'ensemble des régions, chargé de rédiger une convention internationale générale relative à la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles ». Nous ne sommes pas convaincus de la réelle nécessité d'une nouvelle convention internationale relative à la cybercriminalité. Nous sommes en outre très inquiets que le travail de l'ONU dans ce domaine, tel que proposé dans le « Projet de Convention des Nations Unies sur la coopération en matière de lutte contre la cybercriminalité » (A/C.3/72/12) mis en circulation par la Fédération de Russie, ne porte atteinte à l'utilisation de l'internet visant à exercer les droits humains et favoriser le développement social et économique.

Nos préoccupations concernant cette résolution et le processus que celle-ci initierait sont les suivantes :

Tout d'abord, le manque de définition de « l'utilisation des technologies de l'information et des communications à des fins criminelles » dans la résolution. Le texte traite à la fois de questions de cybersécurité (des crimes qui mettent en jeu la « stabilité d'infrastructures essentielles des États et des entreprises ») et des actes criminels commis par le biais des TIC (par exemple, « des trafiquants d'êtres humains […] qui profitent des technologies de l'information et des communications pour mener des activités criminelles »). Un tel manque de spécificité ne pose pas uniquement question du point de vue de l'exactitude ; le fait de ne pas définir ce terme laisse la porte ouverte à la criminalisation de comportements ordinaires en ligne, protégés par les lois internationales relatives aux droits humains.

En second lieu, la criminalisation des activités en ligne habituelles des personnes et des organisations à travers l'application de lois relatives à la cybercriminalité ne cesse d'augmenter dans de nombreux pays du monde. Le Rapporteur spécial de l'ONU sur les droits à la liberté de réunion pacifique et d'association a observé que : « L'adoption massive de lois et de politiques visant à lutter contre la cybercriminalité a en outre ouvert la porte à la répression et à la surveillance des militants et des manifestants dans de nombreux pays. »[1] Comme il le remarque dans son rapport, de telles lois sont utilisées pour : criminaliser l'accès et l'utilisation des communications numériques sécurisées (notamment à travers l'utilisation du chiffrement), des méthodes vitales pour le travail de la société civile, des défenseurs des droits humains (DDH) et des journalistes, ainsi que pour les institutions publiques et privées qui dépendent d'un internet stable et sécurisé ; pour criminaliser des formes légitimes d'expression, d'association et de réunion en ligne en raison de termes vagues et mal définis qui permettent des applications arbitraires ou discrétionnaires et entraînent un flou juridique ; enfin, pour octroyer aux gouvernements ample pouvoir de bloquer des sites Internet jugés critiques envers les autorités, voire des réseaux entiers, des applications et des services qui facilitent les échanges et l'accès à l'information en ligne.

Si la législation peut s'avérer nécessaire pour lutter contre la cybercriminalité et renforcer les institutions démocratiques, en cas de mauvaise utilisation, ces lois sont susceptibles d'engendrer un effet dissuasif et de freiner les capacités des personnes au moment d'utiliser l'internet pour exercer leurs droits en ligne et hors ligne. Comme ont déjà soulevé plusieurs Procédures Spéciales de l'ONU dans leurs communications pour des gouvernements, les lois relatives à la cybercriminalité peuvent engendrer des arrestations et des détentions arbitraires, voire même des morts.[2] L'unique référence

1 Rapport 2019 du Rapporteur spécial sur les droits à la liberté de réunion pacifique et à la liberté d'association (A/HRC/41/41)

2 Arabie Saoudite (SAU 13/2014) Communication des Rapporteurs spéciaux sur la promotion et la protection du droit à la liberté d'opinion et d'expression, sur la liberté de religion ou de croyances, et sur la situation des défenseurs des droits humains, concernant la condamnation de M. Raef Badawi pour « insultes à l'Islam » en vertu de la Loi contre la cybercriminalité ; Bangladesh (BGD 14/2013) Communication du Groupe de travail sur la détention arbitraire, et des Rapporteurs spéciaux sur la promotion et la protection du droit à la liberté d'opinion et d'expression, sur les droits à la liberté de réunion pacifique et à la liberté d'association, et sur la situation des défenseurs des droits humains, concernant la situation de M. Nasiruddin Elan, Directeur d'Odhikar, une organisation non gouvernementale, arrêté pour violation présumée de la Section 57 de la Loi sur les technologies de l'information et des communications et traduit en justice devant le Tribunal de la cybercriminalité ; UAE (ARE 5/2013) Communication des Rapporteurs spéciaux sur la promotion et la protection du droit à la liberté d'opinion et d'expression, sur les droits à la liberté de réunion pacifique et à la liberté d'association, sur la position des défenseurs des droits humains, et sur la torture et autres peines ou traitements cruels, inhumains ou dégradants, concernant l'accusation d'utilisation de la nouvelle Loi de cybercriminalité pour imposer des restrictions injustifiées à la liberté d'expression en ligne ; Iran (IRN 27/2012) Communication du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, le Rapporteur spécial sur la situation des défenseurs des droits humains, le Rapporteur spécial sur la

aux droits humains du projet de résolution, qui réaffirme simplement l'importance du respect des droits humains et des libertés fondamentales dans l'utilisation des TIC, ne suffit pas à garantir les droits humains dans la lutte contre la cybercriminalité.

En troisième lieu, le « Projet de Convention des Nations Unies sur la coopération en matière de lutte contre la cybercriminalité », censé servir de base à la rédaction d'une convention internationale générale, soulève un certain nombre de questions. Il est particulièrement inquiétant que le Projet de Convention propose de dépasser largement ce que permet la Convention de Budapest en matière d'accès transfrontalier aux données, en limitant notamment la possibilité pour un pays signataire de refuser l'octroi de l'accès à des données requises.[3] Le Projet de Convention propose également que l'ONU devienne l'entité d'application avec la création d'un nouvel organe, la Commission technique internationale pour la lutte contre les crimes commis à travers les TIC, parmi d'autres mécanismes d'application. Si un certain nombre de dispositions du Projet de Convention reprennent celles de la Convention de Budapest, les références permettant d'équilibrer les intérêts entre application de la loi et respect des droits humains fondamentaux en sont absentes, tout comme les références au principe de proportionnalité et au droit à l'équité des procédures. Étant donné les efforts de la Fédération de Russie pour élargir le contrôle de son gouvernement sur l'internet avec la loi dite « d'internet souverain » approuvée au début du mois,[4] son rôle de leader pour élaborer un traité international contraignant relatif à la cybercriminalité mérite de faire l'objet d'un examen extrêmement rigoureux.

En quatrième lieu, nous ne sommes pas convaincus de la réelle nécessité d'une nouvelle convention internationale en matière de cybercriminalité. Il serait plus souhaitable et plus pratique de renforcer et améliorer les instruments existants, plutôt que d'allouer des ressources déjà limitées à la réalisation d'un nouveau cadre international, voué à s'étendre sur de nombreuses années et probablement à ne jamais obtenir de consensus. Des sections de l'ONU sont déjà chargées de travailler à la question de la cybercriminalité, spécifiquement l'Office des Nations unies contre la drogue et le crime (ONUDC), et il en est de même aux niveaux national et régional. Selon la base de données de l'ONUDC sur la législation en matière de cybercriminalité,

situation des droits humains en République Islamique d'Iran, le Rapporteur spécial sur les exécutions extrajudiciaires, sommaires ou arbitraires, et le Rapporteur spécial sur la torture et autres peines ou traitements cruels, inhumains ou dégradants, concernant les tortures présumées ayant entrainé la mort de Sattar Beheshti alors qu'il était en détention après son arrestation pour cybercriminalité.

3 Les articles 51-56 du projet de Convention établissent les conditions de disponibilité des données provenant d'autres États. S'ils ne vont pas jusqu'à dire que tous les États devraient avoir l'obligation de transmettre toutes les informations pertinentes, ces articles font largement pression en ce sens pour tous les pays signataires en exigeant la modification de la loi nationale afin de permettre la transmission des données relatives au trafic et au contenu, en vertu des conditions définies dans la convention et des autorisations convenues entre les États.

4 https://www.hrw.org/news/2019/10/31/russia-new-law-expands-government-control-online

plus de 180 pays comportent une législation importante et procédurale en matière de cybercriminalité et de preuves électroniques.[5] Bien entendu, la diversité de la portée des différentes lois nationales reste une question à résoudre, ainsi que la capacité des gouvernements nationaux à les mettre en œuvre. Un processus de l'ONU travaille cependant d'ores et déjà en ce sens. Le Groupe intergouvernemental d'experts à composition non limitée de l'ONU chargé de mener une étude approfondie sur la cybercriminalité devrait publier son rapport en 2021, avec ses résultats et recommandations concernant la législation nationale, les meilleures pratiques, l'assistance technique et la coopération internationale.[6] En outre un processus est actuellement en cours pour élaborer un deuxième protocole additionnel à la Convention de Budapest, l'instrument international le plus largement ratifié en matière de cybercriminalité.[7]

Pour finir, la lutte contre la cybercriminalité se doit d'être une initiative multipartite. Elle suppose la participation des autorités gouvernementales et leurs experts, des membres de la communauté technique, de la société civile, du secteur privé et des institutions scientifiques et de recherche. La mise en place d'un groupe intergouvernemental spécial chargé d'étudier la question de la cybercriminalité exclurait des acteurs dont l'expertise et le point de vue sont précieux, tant pour lutter efficacement contre l'utilisation des TIC à des fins criminelles que pour garantir que de tels efforts ne compromettent pas l'utilisation des TIC dans l'exercice des droits humains et du développement social et économique.

Nous exhortons votre délégation à voter contre la résolution A/C.3/74/L/11/Rev.1 relative à la « Lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles » et à veiller à ce que les initiatives en matière de cybercriminalité tiennent compte de l'ensemble des acteurs.

Cordialement,

7amleh - The Arab Center for the Advancement of Social Media
Access Now
Africa Freedom of Information Centre

5 La base de données contient des extraits de lois pertinentes à des infractions de cybercriminalité et les questions transversales. De plus, elle permet aux utilisateurs d'accéder aux documents complets de la législation.

6 https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-March-2019/Report/UNODC_CCPCJ_EG.4_2019_2_F.pdf

7 La société civile s'engage à élaborer le deuxième protocole additionnel à la Convention de Budapest dans le but de remédier à certaines lacunes de la Convention, et en particulier garantir que les demandes transnationales de données personnelles respectent les protections en matière de droits humains. https://www.eff.org/document/joint-civil-society-response-discussion-guide-2nd-additional-protocol-budapest-convention

Albanian Media Institute
Americans for Democracy & Human Rights in Bahrain
ARTICLE 19
Association pour le progrès des communications (APC)
Bangladesh NGOs Network for Radio and Communication
BlueLink – Bulgarie
Bytes for All (B4A) – Pakistan
Child Rights International Network (CRIN)
Derechos Digitales – Amérique Latine
Digital Rights Foundation
Electronic Frontier Foundation (EFF)
eQuality Project, University of Ottawa – Canada
Fundación Huaira – Quito, Équateur
Fundación Internet Bolivia
Global Partners Digital
Hiperderecho – Pérou
Human Rights in China
Internet Governance Project
Internet Policy Observatory – Pakistan
Internet Society
IPANDETEC – Amérique Central
Jonction – Sénégal
Media Institute of Southern Africa (MISA)
Media Matters for Democracy – Pakistan
Paradigm Initiative – Nigéria
Privacy International
Red en Defensa de los Derechos Digitales (R3D)
Research ICT Africa
Software Freedom Law Center
TEDIC – Paraguay
Usuarios Digitales
Vigilance for Democracy and the Civic State – Tunisie
YMCA Computer Training Centre and Digital Studio – Gambie

Personnes:

(Affiliations listées à des fins d'identification)

Dr. Jennifer Barrigar
Canada

Tamir Israel
Avocat, Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko (CIPPIC)

Douwe Korff
Professeur émérite en droit international, London Metropolitan University et membre associé de l'Oxford Martin School, University of Oxford

Joy Liddicoat
Chercheure, University of Otago, Nouvelle Zélande et vice-présidente de InternetNZ

Damian Loreti
Université de Buenos Aires, Argentine

Valerie Steeves
Professeure titulaire, Département de criminologie, Université d'Ottawa, Canada