22 de diciembre de 2021

Representante Permanente Sra. Faouzia Boumaiza Mebarki, Presidenta

Comité intergubernamental especial de expertos encargado de elaborar una convención internacional integral contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos

Estimada Representante Permanente y Presidenta Sra. Mebarki:

Nosotros, las organizaciones y académicos abajo firmantes, trabajamos para proteger y promover los derechos humanos, tanto en línea como fuera de ella. Los esfuerzos para abordar la ciberdelincuencia nos preocupan, tanto porque la ciberdelincuencia supone una amenaza para los derechos humanos y los medios de vida, como porque las leyes, políticas e iniciativas sobre ciberdelincuencia se utilizan actualmente para socavar los derechos de las personas. Por lo tanto, pedimos que el proceso por el cual el Comité Ad Hoc realiza su trabajo incluya una sólida participación de la sociedad civil a lo largo de todas las etapas de desarrollo y redacción de una convención, y que cualquier propuesta de convención incluya salvaguardias de derechos humanos aplicables tanto a sus disposiciones sustantivas como de procedimiento.

Antecedentes

La propuesta de elaborar una amplia "convención internacional integral sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos" se presenta al mismo tiempo que los mismos mecanismos de derechos humanos de la ONU resalta las alarmas sobre el abuso de las leyes de ciberdelincuencia en todo el mundo. En su informe de 2019, el Relator Especial de la ONU sobre el derecho a la libertad de reunión pacífica y de asociación, Clément Nyaletsossi Voule, observó: "Un aumento de la legislación y las políticas destinadas a combatir la ciberdelincuencia también ha abierto la puerta a castigar y vigilar a activistas y manifestantes en muchos países del mundo." En 2019 y una vez más este año, la Asamblea General de la ONU expresó su grave preocupación por el hecho de que la legislación sobre ciberdelincuencia se esté usando indebidamente para atacar a los defensores de los derechos humanos u obstaculizar su trabajo y poner en peligro su seguridad de manera contraria al derecho internacional. Esto se produce después de años de informes de organizaciones no gubernamentales sobre los abusos de los derechos humanos derivados de las leyes de ciberdelincuencia excesivamente amplias.

Cuando se propuso por primera vez la convención, más de 40 organizaciones y expertos en derechos digitales y derechos humanos, entre ellos muchos de los firmantes de esta carta, instaron a las delegaciones a votar en contra de la resolución, advirtiendo que la convención propuesta supone una amenaza para los derechos humanos.

Antes de la primera sesión del Comité Ad Hoc, reiteramos estas preocupaciones. Si se va a elaborar una convención de las Naciones Unidas sobre la ciberdelincuencia, el

objetivo debe ser combatir el uso de las tecnologías de la información y las comunicaciones con fines delictivos sin poner en peligro los derechos fundamentales de las personas a las que se pretende proteger, para que estas puedan disfrutar y ejercer libremente sus derechos, tanto en línea como fuera de ella. Cualquier propuesta de convenio debe incorporar salvaguardas claras y sólidas en materia de derechos humanos. Una convención sin dichas salvaguardas o que diluya las obligaciones de los Estados en materia de derechos humanos pondría en peligro a las personas y haría que nuestra presencia digital fuera aún más insegura, poniendo en peligro los derechos humanos fundamentales.

A medida que el Comité *Ad Hoc* comience su trabajo de redacción de la convención en los próximos meses, es de vital importancia aplicar un enfoque basado en los derechos humanos para garantizar que el texto propuesto no se utilice como una herramienta para sofocar la libertad de expresión, infringir la privacidad y la protección de datos, o poner en peligro a las personas y comunidades.

La importante labor de combatir la ciberdelincuencia debe ser coherente con las obligaciones de los Estados en materia de derechos humanos establecidas en la Declaración Universal de Derechos Humanos (DUDH), el Pacto Internacional de Derechos Civiles y Políticos (PIDCP) y otros instrumentos y normas internacionales de derechos humanos. En otras palabras, los esfuerzos para combatir la ciberdelincuencia también deben proteger, no socavar, los derechos humanos. Recordamos a los Estados que los mismos derechos que tienen las personas fuera de línea deben protegerse también en línea.

Alcance de las disposiciones penales sustantivas

No existe un consenso sobre cómo abordar la ciberdelincuencia a nivel mundial ni una comprensión o definición común sobre qué constituye la ciberdelincuencia. Desde el punto de vista de los derechos humanos, es esencial que el ámbito de cualquier convención sobre ciberdelincuencia sea reducido. El hecho de que un delito pueda implicar tecnología no significa que deba incluirse en la convención propuesta. Por ejemplo, leyes amplias sobre ciberdelincuencia a menudo, simplemente, añaden penas por el uso de un ordenador o dispositivo en la comisión de un delito existente. Las leyes son especialmente problemáticas cuando incluyen delitos relacionados con el contenido. Las leyes de ciberdelincuencia redactadas de forma imprecisa, que pretenden combatir la desinformación y el apoyo o la glorificación del terrorismo y el extremismo en línea, pueden ser utilizadas de forma indebida para encarcelar a los blogueros o bloquear plataformas enteras en un país determinado. Como tales, no cumplen con las normas internacionales de libertad de expresión. Estas leyes ponen en peligro a periodistas, activistas, investigadores, comunidades LGBTQ y disidentes, y pueden tener un efecto amedrentador en la sociedad en general.

Incluso las leyes que se centran más estrechamente en los delitos relacionados con la informática se emplean para socavar los derechos. Las leyes que penalizan el acceso no autorizado a redes o sistemas informáticos se han usado para elegir como blanco a investigadores de seguridad digital, denunciantes, activistas y periodistas. Con demasiada frecuencia, los investigadores de seguridad, que ayudan a mantener la

seguridad de todos, se ven atrapados en leyes vagas sobre ciberdelincuencia y se enfrentan a cargos penales por identificar fallos en los sistemas de seguridad. Algunos Estados también han interpretado las leyes de acceso no autorizado de forma tan amplia como para criminalizar efectivamente todas y cada una de las denuncias; bajo estas interpretaciones, cualquier revelación de información en violación de una política corporativa o gubernamental podría ser tratada como "ciberdelito". Cualquier convenio potencial debería incluir explícitamente un estándar de intención maliciosa, no debería transformar las políticas de uso de ordenadores corporativos o gubernamentales en responsabilidad penal, debería proporcionar una defensa del interés público claramente articulada y extensa, e incluir disposiciones claras que permitan a los investigadores de seguridad realizar su trabajo sin miedo a ser procesados.

Derechos humanos y garantías procesales

Nuestra información privada y personal, antes encerrada en un cajón del escritorio, reside ahora en nuestros dispositivos digitales y en la nube. La policía de todo el mundo utiliza un conjunto de herramientas de investigación cada vez más intrusivas para acceder a las pruebas digitales. Con frecuencia, sus investigaciones atraviesan las fronteras sin las debidas garantías y eluden las protecciones de los tratados de asistencia jurídica mutua. En muchos contextos, no hay supervisión judicial y el papel de los reguladores independientes de la protección de datos se ve socavado. Las leyes nacionales, incluida la legislación sobre ciberdelincuencia, suelen ser inadecuadas para proteger contra la vigilancia desproporcionada o innecesaria.

Cualquier convenio potencial debería detallar las sólidas salvaguardas procesales y de derechos humanos que rigen las investigaciones penales llevadas a cabo en el marco de dicho convenio. Debe garantizar que cualquier injerencia en el derecho a la intimidad cumpla con los principios de legalidad, necesidad y proporcionalidad, incluso exigiendo una autorización judicial independiente de las medidas de vigilancia. Tampoco debería prohibir a los Estados la adopción de salvaguardas adicionales que limiten los usos de los datos personales por parte de las fuerzas del orden, ya que tal prohibición socavaría la privacidad y la protección de datos. Cualquier convenio potencial debería también reafirmar la necesidad de que los Estados adopten y apliquen "una legislación sólida, robusta y exhaustiva en materia de privacidad, incluida la relativa a la privacidad de los datos, que cumpla con el derecho internacional de los derechos humanos en términos de salvaguardas, supervisión y recursos para proteger efectivamente el derecho a la privacidad. "

Existe un riesgo real de que, en un intento de atraer a todos los Estados para que firmen una propuesta de convención sobre ciberdelincuencia de la ONU, se dé cabida a las malas prácticas en materia de derechos humanos, lo que daría lugar a una carrera a la baja. Por lo tanto, es esencial que cualquier convención potencial refuerce explícitamente las salvaguardas procesales para proteger los derechos humanos y se resista a los atajos en torno a los acuerdos de asistencia mutua.

Participación significativa

De cara al futuro, pedimos al Comité *Ad Hoc* que incluya activamente a las organizaciones de la sociedad civil en las consultas -incluidas las que se ocupan de la seguridad digital y los grupos que ayudan a las comunidades e individuos vulnerables-, lo que no ocurrió cuando este proceso comenzó en 2019 ni en el tiempo transcurrido desde entonces.

En consecuencia, solicitamos al Comité

- Acreditar a los expertos tecnológicos y académicos y a los grupos no gubernamentales interesados, incluidos aquellos con experiencia relevante en derechos humanos, pero que no tienen estatus consultivo en el Consejo Económico y Social de la ONU, de manera oportuna y transparente, y permitir a los grupos participantes registrar a múltiples representantes para acomodar la participación a distancia a través de diferentes zonas horarias.
- Garantizar que las modalidades de participación reconozcan la diversidad de las partes interesadas no gubernamentales, dando a cada grupo interesado un tiempo de intervención adecuado, ya que la sociedad civil, el sector privado y el mundo académico pueden tener opiniones e intereses divergentes.
- Garantizar la participación efectiva de los participantes acreditados, incluyendo la oportunidad de recibir oportunamente los documentos, proporcionar servicios de interpretación, hablar en las sesiones del Comité (en persona y a distancia), y presentar opiniones y recomendaciones por escrito.
- Mantener una página web actualizada y dedicada con información relevante, como información práctica (detalles sobre la acreditación, tiempo/lugar y participación a distancia), documentos de organización (es decir, órdenes del día, documentos de debate, etc.), declaraciones y otras intervenciones de los Estados y otras partes interesadas, documentos de referencia, documentos de trabajo y proyectos de resultados, e informes de reuniones.

La lucha contra la ciberdelincuencia no debe hacerse a expensas de los derechos fundamentales y la dignidad de las personas cuyas vidas se verán afectadas por esta propuesta de convenio. Los Estados deben asegurarse que cualquier propuesta de convenio sobre la ciberdelincuencia esté en consonancia con sus obligaciones en materia de derechos humanos, y deben oponerse a cualquier propuesta de convenio que sea incompatible con dichas obligaciones.

Le agradeceríamos que tuviera la amabilidad de distribuir la presente carta entre los miembros del Comité *Ad Hoc* y publicarla en el sitio web del Comité *Ad Hoc*.

Firmantes,*

1. Access Now – International
2. Alternative ASEAN Network on Burma (ALTSEAN) – Burma
3. Alternatives – Canada
4. Alternative Informatics Association – Turkey
5. AqualtuneLab – Brazil
6. ArmSec Foundation – Armenia

7. ARTICLE 19 – International
8. Asociación por los Derechos Civiles (ADC) – Argentina
9. Asociación Trinidad / Radio Viva – Trinidad
10. Asociatia Pentru Tehnologie si Internet (ApTI) – Romania
11. Association for Progressive Communications (APC) – International
12. Associação Mundial de Rádios Comunitárias (Amarc Brasil) – Brazil
13. ASEAN Parliamentarians for Human Rights (APHR) – Southeast Asia
14. Bangladesh NGOs Network for Radio and Communication (BNNRC) – Bangladesh
15. BlueLink Information Network – Bulgaria
16. Brazilian Institute of Public Law - Brazil
17. Cambodian Center for Human Rights (CCHR) – Cambodia
18. Cambodian Institute for Democracy – Cambodia
19. Cambodia Journalists Alliance Association – Cambodia
20. Casa de Cultura Digital de Porto Alegre – Brazil
21. Centre for Democracy and Rule of Law – Ukraine
22. Centre for Free Expression – Canada
23. Centre for Multilateral Affairs – Uganda
24. Center for Democracy & Technology – United States
25. Civil Society Europe
26. Coalition Direitos na Rede – Brazil
27. Collaboration on International ICT Policy for East and Southern Africa (CIPESA) – Africa
28. CyberHUB-AM – Armenia
29. Data Privacy Brazil Research Association – Brazil
30. Dataskydd – Sweden
31. Derechos Digitales – Latin America
32. Defending Rights & Dissent – United States
33. Digital Citizens – Romania
34. DigitalReach – Southeast Asia
35. Digital Security Lab – Ukraine
36. Državljan D / Citizen D – Slovenia
37. Electronic Frontier Foundation (EFF) – International
38. Electronic Privacy Information Center (EPIC) – United States
39. Elektronisk Forpost Norge – Norway
40. Epicenter.works for digital rights – Austria
41. European Center For Not-For-Profit Law (ECNL) Stichting – Europe
42. European Civic Forum – Europe
43. European Digital Rights (EDRi) – Europe
44. eQuality Project – Canada
45. Fantsuam Foundation – Nigeria
46. Free Speech Coalition – United States

47. Foundation for Media Alternatives (FMA) – Philippines
48. Fundación Acceso – Central America
49. Fundación Ciudadanía y Desarrollo de Ecuador
50. Fundación CONSTRUIR – Bolivia
51. Fundación Karisma – Colombia
52. Fundación OpenlabEC – Ecuador
53. Fundamedios – Ecuador
54. Garoa Hacker Clube – Brazil
55. Global Partners Digital – United Kingdom
56. GreenNet – United Kingdom
57. GreatFire – China
58. Hiperderecho – Peru
59. Homo Digitalis – Greece
60. Human Rights in China – China
61. Human Rights Defenders Network – Sierra Leone
62. Human Rights Watch – International
63. Igarapé Institute -- Brazil
64. IFEX - International
65. Institute for Policy Research and Advocacy (ELSAM) – Indonesia
66. The Influencer Platform – Ukraine
67. INSM Network for Digital Rights – Iraq
68. Internews Ukraine
69. Instituto Beta: Internet & Democracia (IBIDEM) – Brazil
70. Instituto Brasileiro de Defesa do Consumidor (IDEC) – Brazil
71. Instituto Educadigital – Brazil
72. Instituto Nupef – Brazil
73. Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec) – Brazil
74. Instituto de Referência em Internet e Sociedade (IRIS) – Brazil
75. Instituto Panameño de Derecho y Nuevas Tecnologías (IPANDETEC) – Panama
76. Instituto para la Sociedad de la Información y la Cuarta Revolución Industrial – Peru
77. International Commission of Jurists – International
78. The International Federation for Human Rights (FIDH)
79. IT-Pol – Denmark
80. JCA-NET – Japan
81. KICTANet – Kenya
82. Korean Progressive Network Jinbonet – South Korea
83. Laboratorio de Datos y Sociedad (Datysoc) – Uruguay
84. Laboratório de Políticas Públicas e Internet (LAPIN) – Brazil
85. Latin American Network of Surveillance, Technology and Society Studies (LAVITS)

86. Lawyers Hub Africa
87. Legal Initiatives for Vietnam
88. Ligue des droits de l'Homme (LDH) – France
89. Masaar - Technology and Law Community – Egypt
90. Manushya Foundation – Thailand
91. MINBYUN Lawyers for a Democratic Society – Korea
92. Open Culture Foundation – Taiwan
93. Open Media – Canada
94. Open Net Association – Korea
95. OpenNet Africa – Uganda
96. Panoptykon Foundation – Poland
97. Paradigm Initiative – Nigeria
98. Privacy International – International
99. Radio Viva – Paraguay
100. Red en Defensa de los Derechos Digitales (R3D) – Mexico
101. Regional Center for Rights and Liberties – Egypt
102. Research ICT Africa
103. Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC) – Canada
104. Share Foundation - Serbia
105. Social Media Exchange (SMEX) – Lebanon, Arab Region
106. SocialTIC – Mexico
107. Southeast Asia Freedom of Expression Network (SAFEnet) – Southeast Asia
108. Supporters for the Health and Rights of Workers in the Semiconductor Industry (SHARPS) – South Korea
109. Surveillance Technology Oversight Project (STOP) – United States
110. Tecnología, Investigación y Comunidad (TEDIC) – Paraguay
111. Thai Netizen Network – Thailand
112. Unwanted Witness – Uganda
113. Vrijschrift – Netherlands
114. West African Human Rights Defenders Network – Togo
115. World Movement for Democracy – International
116. 7amleh – The Arab Center for the Advancement of Social Media – Arab Region

Individual Experts and Academics

1. Jacqueline Abreu, University of São Paulo
2. Chan-Mo Chung, Professor, Inha University School of Law
3. Danilo Doneda, Brazilian Institute of Public Law

4. David Kaye, Clinical Professor of Law, UC Irvine School of Law, former UN Special Rapporteur on Freedom of Opinion and Expression (2014-2020)
5. Wolfgang Kleinwächter, Professor Emeritus, University of Aarhus; Member, Global Commission on the Stability of Cyberspace
6. Douwe Korff**,** Emeritus Professor of International Law**,** London Metropolitan University
7. Fabiano Menke, Federal University of Rio Grande do Sul
8. Kyung-Sin Park, Professor, Korea University School of Law
9. Christopher Parsons, Senior Research Associate, Citizen Lab, Munk School of Global Affairs & Public Policy at the University of Toronto
10. Marietje Schaake, Stanford Cyber Policy Center
11. Valerie Steeves, J.D., Ph.D., Full Professor, Department of Criminology University of Ottawa

Lista de firmantes al 13 de enero de 2022