22 de dezembro de 2021

V. Ex. Sra. Faouzia Boumaiza Mebarki
Presidente

Comitê Ad Hoc para Elaboração de Convenção Internacional sobre o Uso de Tecnologias de Informação e Comunicação para Fins Criminais

United Nations Office on Drugs and Crime (UNODC)
UNODC New York Office
United Nations Headquarters
DC1 Building
Room 613
One United Nations Plaza
New York, NY 10017

Vossa Excelência,

Nós, organizações subscritas abaixo, trabalhamos para proteger e ampliar direitos humanos, online e offline. Esforços para tratar de crimes cibernéticos são uma preocupação nossa, tanto por crimes cibernéticos representarem uma ameaça a direitos e à dignidade humana, quanto por leis, políticas e iniciativas sobre tais crimes serem constantemente utilizadas para enfraquecer direitos fundamentais. Portanto, pedimos que o Comitê Ad Hoc inclua, de forma robusta, a participação da sociedade civil em todo o processo de seus trabalhos para o desenvolvimento e elaboração da convenção e que qualquer proposta de texto inclua salvaguardas aos direitos humanos aplicáveis a disposições materiais e procedimentais.

Panorama geral

A proposta de elaboração de uma "Convenção Internacional sobre o Uso de Tecnologias de Informação e Comunicação para Fins Criminais" está sendo apresentada ao mesmo tempo em que mecanismos de direitos humanos da ONU chamam a atenção para o abuso presente em leis de crimes cibernéticos ao redor do mundo.

Em seu relatório de 2019, o relator especial dos direitos de liberdade de reunião e associação das Nações Unidas, Clément Nyaletsossi Voule, observou que "um aumento de legislações e políticas de combate a crimes cibernéticos também abriu portas para a punição e vigilância de ativistas e manifestantes em vários países ao redor do mundo". Em 2019 e novamente neste ano, a Assembleia Geral da ONU expressou grande preocupação em relação às legislações sobre crimes cibernéticos estarem sendo utilizadas de forma inadequada para atingir defensores de direitos humanos ou impedir seu trabalho e colocar em risco a segurança contrariando as normas internacionais. Isso é resultado de

anos de denúncias feitas por organizações não governamentais sobre os abusos contra direitos fundamentais decorrentes de leis sobre crimes cibernéticos.

Quando a convenção foi proposta pela primeira vez, mais de 40 das principais organizações e especialistas de direitos digitais e direitos humanos, incluindo vários dos signatários desta carta, instaram as delegações a votar contra a resolução, alertando que a convenção proposta é uma ameaça aos direitos humanos.

Antes da primeira sessão do Comitê Ad Hoc, nós reiteramos estas preocupações. Se a convenção da ONU sobre crimes cibernéticos proceder, o objetivo deve ser o combate ao uso de tecnologias de informação e comunicação para fins criminais sem prejudicar os direitos fundamentais daqueles que se pretende proteger, para que as pessoas possam livremente gozar e exercer seus direitos, *online e offline*. Qualquer proposta de convenção deve incorporar salvaguardas de direitos humanos claras e robustas. Uma convenção sem tais salvaguardas, ou que dilua as obrigações estatais em relação aos direitos humanos, colocaria os indivíduos em risco e tornaria nossa presença digital ainda mais insegura, ameaçando direitos fundamentais em ambos os casos.

À medida que o Comitê Ad Hoc inicia o seu trabalho para a elaboração da convenção nos próximos meses, é vital que seja seguida uma abordagem baseada em direitos humanos para garantir que a proposta de texto não seja utilizada como ferramenta para reprimir a liberdade de expressão, violar a privacidade e a proteção de dados ou ameaçar indivíduos e comunidades em risco.

O importante trabalho de combater os crimes cibernéticos deve ser consistente com as obrigações estatais em matéria de direitos humanos definidas na Declaração Universal de Direitos Humanos, no Pacto Internacional sobre Direitos Civis e Políticos e outros instrumentos e normas internacionais de direitos humanos. Em outras palavras, esforços para combater crimes cibernéticos devem também proteger, e não debilitar, os direitos humanos. Reforça-se aos Estados que os mesmos direitos que um indivíduo tem offline devem ser protegidos online.

Escopo das Disposições Criminais Materiais

Não há consenso quanto a como enfrentar os crimes cibernéticos a nível global, nem há um entendimento comum ou definição sobre o que se constitui como crime cibernético. Da perspectiva dos direitos humanos, é essencial manter restrito o escopo de qualquer convenção sobre crimes cibernéticos. Isto é, não é porque um crime envolve tecnologia que ele necessariamente deve ser incluído na convenção. Por exemplo, normas mais amplas sobre crimes cibernéticos muitas vezes estabelecem novas penalidades simplesmente em razão da utilização de um computador ou dispositivo na prática de um delito já existente. As normas são especialmente problemáticas quando incluem conteúdo relacionado a crimes. Leis sobre crimes cibernéticos com texto vago, que pretendem combater a desinformação e o apoio ou apologia online ao terrorismo e extremismo, podem ser usadas para prender blogueiros ou bloquear plataformas inteiras em certos países. Deste modo, elas falham em atender aos padrões internacionais de liberdade de

expressão. Tais leis colocam jornalistas, ativistas, pesquisadores, membros da comunidade LGBTQIA+ e dissidentes em risco e podem ter um efeito assustador na sociedade como um todo.

Mesmo leis que focam de maneira mais estreita no núcleo tradicional de crimes cibernéticos são utilizadas para reduzir direitos. Leis que criminalizam o acesso não autorizado a computadores e sistemas têm sido usadas para atacar pesquisadores de segurança, denunciantes, ativistas e jornalistas. Frequentemente, pesquisadores de segurança, que ajudam a manter todos seguros, são enquadrados por leis de crimes cibernéticos vagas e enfrentam acusações criminais por terem identificado falhas na segurança de sistemas. Alguns Estados também interpretam leis sobre o acesso não autorizado de forma tão ampla que, na prática, criminalizam todo e qualquer denunciante; sob esta interpretação, qualquer divulgação de informações que violem políticas corporativas ou estatais pode ser tratada como "crime cibernético". Uma futura convenção deve explicitamente incluir um requisito de intenção maliciosa, não deve transformar políticas de uso de computadores corporativos e estatais em responsabilidade criminal, deve ser articulada de forma clara e promover a ampla defesa do interesse público, assim como incluir disposições claras que permitam que pesquisadores de segurança executem seu trabalho sem medo de serem processados.

Direitos Humanos e Salvaguardas Processuais

Nossas informações pessoais e privadas, antes trancadas em uma gaveta, agora encontram-se em dispositivos digitais e na nuvem. A polícia ao redor do mundo utiliza um conjunto de ferramentas investigativas cada vez mais intrusivas para acessar provas digitais. Frequentemente, suas investigações atravessam fronteiras sem salvaguardas adequadas e não observam proteções de tratados de assistência jurídica mútua. Em muitos contextos, não há nenhum controle judicial e o papel de reguladores independentes de proteção de dados é enfraquecido. Normas nacionais, incluindo as de crimes cibernéticos, são frequentemente inadequadas para proteger contra vigilância desnecessária e desproporcional.

Uma futura convenção deve detalhar robustas salvaguardas processuais e de direitos humanos que orientem investigações criminais conduzidas sob o escopo da convenção. Ela deve assegurar que qualquer interferência ao direito à privacidade atenda aos princípios da legalidade, necessidade e proporcionalidade, inclusive por meio da exigência de autorização judicial independente para medidas de vigilância. Ela também não deve impedir os Estados de adotarem salvaguardas adicionais que limitem o uso de dados pessoais pelas autoridades policiais, uma vez que esta proibição comprometeria a privacidade e a proteção de dados. Uma futura convenção deve reafirmar a necessidade de Estados adotarem e imporem "legislações de privacidade fortes, robustas e abrangentes, inclusive sobre proteção de dados, que atendam às normas internacionais de direitos humanos quanto a salvaguardas, fiscalização e remédios para proteger o direito à privacidade de forma eficaz".

Existe um risco real de que, ao tentar convencer todos os Estados a assinarem a proposta de convenção sobre crimes cibernéticos da ONU, práticas ruins quanto aos direitos humanos sejam normalizadas, nivelando por baixo as garantias exigidas e deteriorando a proteção do indivíduo. Portanto, é essencial que uma futura convenção reforce explicitamente as salvaguardas processuais voltadas à proteção dos direitos humanos e resista a tentativas de contornar acordos de assistência mútua.

Participação Significativa

Ante o exposto, pedimos ao Comitê Ad Hoc que inclua ativamente as organizações da sociedade civil em processos de consulta – incluindo aquelas que tratam de segurança digital e grupos de assistência a comunidades e indivíduos vulnerabilizados –, o que não ocorreu quando o processo começou em 2019 ou em qualquer outro momento desde então.

Assim, requeremos que o Comitê:

- Credencie especialistas acadêmicos e da área de tecnologia, e organizações não governamentais interessadas, incluindo aqueles com expertise relevante em direitos humanos, mas que não têm status consultivo no Conselho Econômico e Social da ONU, em tempo hábil e de forma transparente, e permita que os grupos participantes registrem múltiplos representantes para possibilitar a participação remota em diversos fuso-horários.

- Garanta que as modalidades de participação reconheçam a diversidade de atores não governamentais, dando a cada grupo interessado tempo adequado de fala, considerando que a sociedade civil, setor privado e academia podem ter visões e interesses distintos.

- Garanta a participação efetiva de participantes credenciados, incluindo a oportunidade de receber em tempo oportuno acesso a documentos, providenciar serviços de tradução e falar nas sessões do Comitê (pessoal ou remotamente), e submeter por escrito notas técnicas e recomendações.

- Manter atualizada uma página online dedicada a informações relevantes, como informações práticas (detalhes sobre o credenciamento, horário/localização, e participações remotas), documentos organizacionais (i.e., agendas, documentos de discussão, etc.), depoimentos e outras intervenções feitas por Estados e outros atores, documentos de referência, documentos de trabalho, rascunhos e atas de reuniões.

O combate aos crimes cibernéticos não deveria prejudicar os direitos fundamentais e a dignidade das pessoas que serão impactadas pela convenção. Os Estados devem garantir que uma futura convenção sobre crimes cibernéticos esteja alinhada com suas obrigações de direitos humanos e devem se opor a qualquer proposta que seja inconsistente com tais obrigações.

Apreciamos fortemente se puder circular a presente carta aos membros do Comitê Ad Hoc e publicá-la no site do Comitê.

Signatários,*

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. Center for Justice and International Law (CEJIL) - International
26. Centro de Estudios en Libertad de Expresión y Acceso (CELE) – Argentina
27. Civil Society Europe
28. Coalition Direitos na Rede – Brazil
29. Código Sur - Costa Rica
30. Collaboration on International ICT Policy for East and Southern Africa (CIPESA) – Africa
31. CyberHUB-AM – Armenia
32. Data Privacy Brazil Research Association – Brazil
33. Dataskydd – Sweden
34. Derechos Digitales – Latin America
35. Defending Rights & Dissent – United States
36. Digital Citizens – Romania
37. DigitalReach – Southeast Asia
38. Digital Rights Watch - Australia

39. Digital Security Lab – Ukraine
40. Državljan D / Citizen D – Slovenia
41. Electronic Frontier Foundation (EFF) – International
42. Electronic Privacy Information Center (EPIC) – United States
43. Elektronisk Forpost Norge – Norway
44. Epicenter.works for digital rights – Austria
45. European Center For Not-For-Profit Law (ECNL) Stichting – Europe
46. European Civic Forum – Europe
47. European Digital Rights (EDRi) – Europe
48. eQuality Project – Canada
49. Fantsuam Foundation – Nigeria
50. Free Speech Coalition – United States
51. Foundation for Media Alternatives (FMA) – Philippines
52. Fundación Acceso – Central America
53. Fundación Ciudadanía y Desarrollo de Ecuador
54. Fundación CONSTRUIR – Bolivia
55. Fundacion Datos Protegidos – Chile
56. Fundación EsLaRed de Venezuela
57. Fundación Karisma – Colombia
58. Fundación OpenlabEC – Ecuador
59. Fundamedios – Ecuador
60. Garoa Hacker Clube – Brazil
61. Global Partners Digital – United Kingdom
62. GreenNet – United Kingdom
63. GreatFire – China
64. Hiperderecho – Peru
65. Homo Digitalis – Greece
66. Human Rights in China – China
67. Human Rights Defenders Network – Sierra Leone
68. Human Rights Watch – International
69. ICT4Peace Foundation – Switzerland
70. Igarapé Institute – Brazil
71. IFEX - International
72. Institute for Policy Research and Advocacy (ELSAM) – Indonesia
73. The Influencer Platform – Ukraine
74. INSM Network for Digital Rights – Iraq
75. Internews Ukraine
76. InternetNZ – New Zealand
77. Instituto Beta: Internet & Democracia (IBIDEM) – Brazil
78. Instituto Brasileiro de Defesa do Consumidor (IDEC) – Brazil
79. Instituto Educadigital – Brazil
80. Instituto Nupef – Brazil
81. Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec) – Brazil
82. Instituto de Referência em Internet e Sociedade (IRIS) – Brazil
83. Instituto Panameño de Derecho y Nuevas Tecnologías (IPANDETEC) – Panama

84. Instituto para la Sociedad de la Información y la Cuarta Revolución Industrial – Peru
85. International Commission of Jurists – International
86. The International Federation for Human Rights (FIDH) – International
87. Irish Council for Civil Liberties (ICCL) – Ireland
88. IT-Pol – Denmark
89. JCA-NET – Japan
90. KICTANet – Kenya
91. Korean Progressive Network Jinbonet – South Korea
92. Laboratorio de Datos y Sociedad (Datysoc) – Uruguay
93. Laboratório de Políticas Públicas e Internet (LAPIN) – Brazil
94. Latin American Network of Surveillance, Technology and Society Studies (LAVITS)
95. Lawyers Hub Africa
96. Legal Initiatives for Vietnam
97. Ligue des droits de l'Homme (LDH) – France
98. Masaar - Technology and Law Community – Egypt
99. Manushya Foundation – Thailand
100. MINBYUN Lawyers for a Democratic Society - Korea
101. Open Culture Foundation – Taiwan
102. Open Media – Canada
103. Open Net Association – Korea
104. OpenNet Africa – Uganda
105. Panoptykon Foundation – Poland
106. Paradigm Initiative – Nigeria
107. Privacy International – International
108. Radio Viva – Paraguay
109. Red en Defensa de los Derechos Digitales (R3D) – Mexico
110. Regional Center for Rights and Liberties – Egypt
111. Research ICT Africa
112. Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC) – Canada
113. Share Foundation - Serbia
114. Social Media Exchange (SMEX) – Lebanon, Arab Region
115. SocialTIC – Mexico
116. Southeast Asia Freedom of Expression Network (SAFEnet) – Southeast Asia
117. Supporters for the Health and Rights of Workers in the Semiconductor Industry (SHARPS) – South Korea
118. Surveillance Technology Oversight Project (STOP) – United States
119. Tecnología, Investigación y Comunidad (TEDIC) – Paraguay
120. Thai Netizen Network – Thailand
121. Unwanted Witness – Uganda
122. Vrijschrift – Netherlands
123. West African Human Rights Defenders Network – Togo
124. World Movement for Democracy – International

125. 7amleh – The Arab Center for the Advancement of Social Media – Arab Region

Os especialistas individuais e acadêmicos

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

**List of signatories as of March 10, 2022*