22. Dezember 2021

Exzellenz Frau Faouzia Boumaiza Mebarki

Vorsitzende

Ad-hoc-Ausschuss zur Ausarbeitung eines umfassenden internationalen Übereinkommens zur Bekämpfung des Einsatzes von Informations- und Kommunikationstechnologien zu kriminellen Zwecken

Exzellenz,

Wir, die unterzeichnenden Organisationen und Akademiker*innen, setzen uns für den Schutz und die Förderung der Menschenrechte ein, online und offline. Die Bemühungen zur Bekämpfung von Cyberkriminalität sind uns ein Anliegen, sowohl weil Cyberkriminalität eine Bedrohung für die Menschenrechte und den Lebensunterhalt darstellt, als auch weil Gesetze, Strategien und Initiativen zur Cyberkriminalität derzeit dazu genutzt werden, die Rechte der Menschen zu untergraben. Wir fordern daher, dass der Prozess, in dem der Ad-hoc-Ausschuss seine Arbeit verrichtet, eine solide Beteiligung der Zivilgesellschaft in allen Phasen der Entwicklung und des Entwurfs einer Konvention vorsieht und dass jede vorgeschlagene Konvention Menschenrechtsgarantien enthält, die sowohl für die materiellen als auch für die verfahrensrechtlichen Bestimmungen gelten.

Hintergrund

Der Vorschlag zur Ausarbeitung eines umfassenden „internationalen Übereinkommens über die Bekämpfung der Nutzung von Informations- und Kommunikationstechnologien zu kriminellen Zwecken“ wird zur gleichen Zeit vorgelegt, in der die Menschenrechtsmechanismen der Vereinten Nationen vor dem Missbrauch von Gesetzen zur Internetkriminalität in der ganzen Welt warnen. Der UN-Sonderberichterstatter für das Recht auf friedliche Versammlungs- und Vereinigungsfreiheit, Clément Nyaletsossi Voule, stellt in seinem Bericht für 2019 fest: „Ein Anstieg der Gesetzgebung und der politischen Maßnahmen zur Bekämpfung der Internetkriminalität hat in vielen Ländern der Welt auch die Tür zur Bestrafung und Überwachung von Aktivist*innen und Demonstrant*innen geöffnet.“

2019 und auch in diesem Jahr hat die UN-Generalversammlung ihre große Besorgnis darüber zum Ausdruck gebracht, dass Gesetze zur Cyberkriminalität missbraucht werden, um Menschenrechtsverteidiger*innen ins Visier zu nehmen oder ihre Arbeit zu behindern und ihre Sicherheit in einer Weise zu gefährden, die dem Völkerrecht zuwiderläuft. Dies ist das Ergebnis jahrelanger Berichte von Nichtregierungsorganisationen über die Menschenrechtsverletzungen, die sich aus zu weit gefassten Gesetzen zur Internetkriminalität ergeben.

Als die Konvention zum ersten Mal vorgeschlagen wurde, forderten über 40 führende Organisationen und Expert*innen für digitale Rechte und Menschenrechte, darunter viele Unterzeichner*innen dieses Schreibens, die Delegationen auf, gegen die Resolution zu stimmen und warnten davor, dass die vorgeschlagene Konvention eine Gefahr für die Menschenrechte darstellt.

Im Vorfeld der ersten Sitzung des Ad-hoc-Ausschusses bekräftigen wir diese Bedenken. Wenn eine UN-Konvention über Cyberkriminalität ausgearbeitet werden soll, sollte das Ziel darin bestehen, die Nutzung von Informations- und Kommunikationstechnologien für kriminelle Zwecke zu bekämpfen – ohne die Grundrechte derjenigen zu gefährden, die sie schützen soll, damit die Menschen ihre Rechte online und offline frei genießen und ausüben können. Jede vorgeschlagene Konvention sollte klare und starke Menschenrechtsgarantien enthalten. Ein Übereinkommen ohne solche Garantien, welches die Menschenrechtsverpflichtungen der Staaten verwässert, würde den Einzelnen in Gefahr bringen und unsere digitale Präsenz noch unsicherer machen. Beides bedeutet eine Bedrohung der grundlegenden Menschenrechte.

Wenn der Ad-hoc-Ausschuss in den kommenden Monaten mit der Ausarbeitung des Übereinkommens beginnt, ist es von entscheidender Bedeutung, einen menschenrechtsbasierten Ansatz zu verfolgen, um sicherzustellen, dass der vorgeschlagene Text nicht als Instrument zur Unterdrückung der Meinungsfreiheit, zur Verletzung der Privatsphäre und des Datenschutzes oder zur Gefährdung von Einzelpersonen und Gemeinschaften eingesetzt wird.

Die wichtige Aufgabe der Bekämpfung der Cyberkriminalität sollte mit den Menschenrechtsverpflichtungen der Staaten in Einklang stehen, die in der Allgemeinen Erklärung der Menschenrechte (AEMR/UDHR engl.), dem Internationalen Pakt über bürgerliche und politische Rechte (IPBPR/ICCPR engl.) und anderen internationalen Menschenrechtsinstrumenten und -standards niedergelegt sind. Mit anderen Worten: Die

Bemühungen zur Bekämpfung von Internetkriminalität sollten auch die Menschenrechte schützen und nicht untergraben. Wir erinnern die Staaten daran, dass dieselben Rechte, die der Einzelne offline hat, auch online geschützt werden sollten.

Anwendungsbereich der wesentlichen, strafrechtlichen Bestimmungen

Es gibt weder einen Konsens darüber, wie Cyberkriminalität auf globaler Ebene bekämpft werden soll, noch ein gemeinsames Verständnis oder eine Definition dessen, was Cyberkriminalität ist. Aus menschenrechtlicher Sicht ist es wichtig, den Geltungsbereich eines Übereinkommens über Cyberkriminalität eng zu halten. Nur weil ein Verbrechen möglicherweise mit Technologie verbunden ist, muss es nicht in die vorgeschlagene Konvention aufgenommen werden. So werden beispielsweise in weitreichenden Gesetzen zur Cyberkriminalität häufig nur Strafen für die Verwendung eines Computers oder Geräts bei der Begehung einer bestehenden Straftat hinzugefügt. Diese Gesetze sind besonders problematisch, wenn sie inhaltsbezogene Straftaten einschließen. Vage formulierte Gesetze zur Cyberkriminalität, die vorgeben, Fehlinformationen („Fake News“) und die Online-Unterstützung oder Verherrlichung von Terrorismus und Extremismus zu bekämpfen, können dazu missbraucht werden, Blogger*innen zu inhaftieren oder ganze Plattformen in einem bestimmten Land zu sperren. Als solche entsprechen sie nicht den internationalen Standards für das Recht auf freie Meinungsäußerung. Solche Gesetze bringen Journalist*innen, Aktivist*innen, Forschende, LGBTQ-Personen und Andersdenkende in Gefahr und können eine abschreckende Wirkung auf die Gesellschaft im Allgemeinen haben.

Auch Gesetze, die sich enger auf cyber-gestützte Straftaten konzentrieren, werden zur Untergrabung von Rechten eingesetzt. Gesetze, die den unbefugten Zugang zu Computernetzwerken oder -systemen unter Strafe stellen, wurden genutzt, um digitale Sicherheitsforschende, Whistleblower, Aktivist*innen und Journalist*innen ins Visier zu nehmen. Allzu oft geraten Sicherheitsforschende, die zum Schutz aller beitragen, in die Fänge vager Gesetze zur Cyberkriminalität und werden strafrechtlich verfolgt, weil sie Schwachstellen in Sicherheitssystemen aufgedeckt haben. Einige Staaten haben die Gesetze über den unerlaubten Zugang so weit ausgelegt, dass sie praktisch jedes Whistleblowing kriminalisieren; nach dieser Auslegung könnte jede Weitergabe von Informationen, die gegen Unternehmens- oder Regierungsrichtlinien verstößt, als „Cyberkriminalität“ behandelt werden. Jedes potenzielle Übereinkommen sollte ausdrücklich einen Standard für böswillige Absicht enthalten, sollte drei Anliegen berücksichtigen: Erstens, sollte es die Richtlinien von Unternehmen oder Regierungen zur Computernutzung nicht in eine strafrechtliche Haftung umwandeln. Zweitens, sollte eine klar

formulierte und weitreichende Verteidigung des öffentlichen Interesses vorsehen. Und drittens, sollte es klare Bestimmungen enthalten, die es Sicherheitsforscher*innen ermöglichen, ihre Arbeit ohne Angst vor Strafverfolgung zu tun.

Menschenrechte und Verfahrensgarantien

Unsere privaten und persönlichen Daten, die früher in einer Schreibtischschublade lagerten, befinden sich heute auf unseren digitalen Geräten und in der Cloud. Weltweit setzt die Polizei immer mehr Ermittlungsinstrumente ein, um auf digitale Beweise zuzugreifen. Häufig werden ihre Ermittlungen grenzüberschreitend ohne angemessene Schutzmaßnahmen durchgeführt und die Schutzbestimmungen von Rechtshilfeverträgen umgangen. In vielen Fällen findet keine richterliche Aufsicht statt, und die Rolle unabhängiger Datenschutzbehörden wird untergraben. Nationale Gesetze, einschließlich der Gesetze zur Cyberkriminalität, sind oft unzureichend, um vor unverhältnismäßiger oder unnötiger Überwachung zu schützen.

Ein mögliches Übereinkommen sollte solide Verfahrens- und Menschenrechtsgarantien für strafrechtliche Ermittlungen im Rahmen eines solchen Übereinkommens enthalten. Es sollte sicherstellen, dass jeder Eingriff in das Recht auf Privatsphäre den Grundsätzen der Rechtmäßigkeit, Notwendigkeit und Verhältnismäßigkeit entspricht, unter anderem durch die Forderung nach einer unabhängigen richterlichen Genehmigung von Überwachungsmaßnahmen. Es sollte den Staaten auch nicht verbieten, zusätzliche Schutzmaßnahmen zu ergreifen, die die Verwendung personenbezogener Daten durch die Strafverfolgungsbehörden einschränken, da ein solches Verbot die Privatsphäre und den Datenschutz untergraben würde. Ein mögliches Übereinkommen sollte auch bekräftigen, dass die Staaten „starke, robuste und umfassende Rechtsvorschriften zum Schutz der Privatsphäre, einschließlich des Datenschutzes, verabschieden und durchsetzen müssen, die mit den internationalen Menschenrechtsnormen in Bezug auf Schutzmaßnahmen, Aufsicht und Rechtsmittel in Einklang stehen, um das Recht auf Privatsphäre wirksam zu schützen."

Es besteht die reale Gefahr, dass in dem Versuch, alle Staaten zur Unterzeichnung eines vorgeschlagenen UN-Übereinkommens über Cyberkriminalität zu bewegen, schlechte Menschenrechtspraktiken berücksichtigt werden – das sogenannte „*race to the bottom*". Daher ist es von entscheidender Bedeutung, dass jede potenzielle Konvention ausdrücklich die Verfahrensgarantien zum Schutz der Menschenrechte stärkt und Abkürzungen über Rechtshilfeabkommen ablehnt.

Sinnvolle Beteiligung

Wir fordern den Ad-hoc-Ausschuss auf, in Zukunft aktiv zivilgesellschaftliche Organisationen in die Konsultationen einzubeziehen – einschließlich derjenigen, die sich mit digitaler Sicherheit befassen, und Gruppen, die gefährdete Gemeinschaften und Einzelpersonen unterstützen –, was weder zu Beginn dieses Prozesses im Jahr 2019 noch in der Zwischenzeit geschehen ist.

Daher fordern wir den Ausschuss zu folgenden Maßnahmen auf:

● Akkreditierung interessierter, akademischer und IT-Expert*innen, sowie nichtstaatliche Gruppen, einschließlich solcher mit einschlägigem Fachwissen im Bereich der Menschenrechte, die bisher keinen beratenden Status beim Wirtschafts- und Sozialrat der Vereinten Nationen haben. Dies sollte rechtzeitig und auf transparente Weise geschehen. Die Registrierung mehrerer Vertreter*innen der verschiedenen Gruppen sollte ermöglicht werden, um die Fernteilnahme über verschiedene Zeitzonen hinweg zu gewährleisten.

● Die Modalitäten für die Teilnahme sollten die Vielfalt der nichtstaatlichen Interessengruppen abbilden. Jede Interessengruppe sollte eine angemessene Redezeit eingeräumt werden, da die Zivilgesellschaft, der Privatsektor und die Wissenschaft unterschiedliche Ansichten und Interessen haben können.

● Sicherstellung einer effektiven Beteiligung von akkreditierten Teilnehmer*innen, einschließlich der Möglichkeit, rechtzeitig Zugriff zu Dokumenten zu erhalten, Dolmetscherdienste bereitzustellen, auf den Ausschusssitzungen (persönlich und aus der Ferne) zu sprechen und schriftliche Stellungnahmen und Empfehlungen einzureichen.

● Pflege einer aktuellen, eigens eingerichteten Webseite mit relevanten Informationen, einschließlich praktischer Informationen (Einzelheiten zur Akkreditierung, Zeit/Ort und Fernteilnahme), organisatorische Dokumente (d.h. Tagesordnungen, Diskussionsunterlagen usw.), Erklärungen und andere Beiträge von Staaten und anderen Interessengruppen, Hintergrunddokumente, Arbeitsunterlagen und Entwürfe von Ergebnissen sowie Sitzungsberichten.

Die Bekämpfung der Cyberkriminalität darf nicht auf Kosten der Grundrechte und der Würde derjenigen gehen, deren Leben durch das vorgeschlagene Übereinkommen berührt wird. Die Staaten sollten sicherstellen, dass jede vorgeschlagene Konvention zur Cyberkriminalität mit

ihren Menschenrechtsverpflichtungen im Einklang steht, und sie sollten sich jeder vorgeschlagenen Konvention widersetzen, die mit diesen Verpflichtungen unvereinbar ist.

Wir wären Ihnen sehr dankbar, wenn Sie das vorliegende Schreiben an die Mitglieder des Ad-hoc-Ausschusses weiterleiten und auf der Website des Ad-hoc-Ausschusses veröffentlichen könnten.

Unterzeichnende*

1. Access Now – International
2. Alternative ASEAN Network on Burma (ALTSEAN) – Myanmar
3. Alternatives – Kanada
4. Alternative Informatics Association – Turkei
5. AqualtuneLab – Brasilien
6. ArmSec Foundation – Armenien
7. ARTICLE 19 – International
8. Asociación por los Derechos Civiles (ADC) – Argentinien
9. Asociación Trinidad / Radio Viva – Trinidad
10. Asociatia Pentru Tehnologie si Internet (ApTI) – Rumänien
11. Association for Progressive Communications (APC) – International
12. Associação Mundial de Rádios Comunitárias (Amarc Brasil) – Brasilien
13. ASEAN Parliamentarians for Human Rights (APHR) – Südostasien
14. Bangladesh NGOs Network for Radio and Communication (BNNRC) – Bangladesch
15. BlueLink Information Network – Bulgarien
16. Brazilian Institute of Public Law - Brasilien

17. Cambodian Center for Human Rights (CCHR) – Kambodscha
18. Cambodian Institute for Democracy – Kambodscha
19. Cambodia Journalists Alliance Association – Kambodscha
20. Casa de Cultura Digital de Porto Alegre – Brasilien
21. Centre for Democracy and Rule of Law – Ukraine
22. Centre for Free Expression – Kanada
23. Centre for Multilateral Affairs – Uganda
24. Center for Democracy & Technology – USA
25. Civil Society Europe
26. Coalition Direitos na Rede – Brasilien
27. Collaboration on International ICT Policy for East and Southern Africa (CIPESA) – Afrika
28. CyberHUB-AM – Armenien
29. Data Privacy Brazil Research Association – Brasilien
30. Dataskydd – Schweden
31. Derechos Digitales – Lateinamerika
32. Defending Rights & Dissent – USA
33. Digital Citizens – Rumänien
34. DigitalReach – Südostasien
35. Digital Security Lab – Ukraine
36. Državljan D / Citizen D – Slowenien
37. Electronic Frontier Foundation (EFF) – International
38. Electronic Privacy Information Center (EPIC) – USA
39. Elektronisk Forpost Norge – Norwegen
40. Epicenter.works for digital rights – Österreich

41. European Center For Not-For-Profit Law (ECNL) Stichting – Europa
42. European Civic Forum – Europa
43. European Digital Rights (EDRi) – Europa
44. eQuality Project – Kanada
45. Fantsuam Foundation – Nigeria
46. Free Speech Coalition – USA
47. Foundation for Media Alternatives (FMA) – Philippinen
48. Fundación Acceso – Zentralamerika
49. Fundación Ciudadanía y Desarrollo de Ecuador
50. Fundación CONSTRUIR – Bolivien
51. Fundación Karisma – Kolumbien
52. Fundación OpenlabEC – Equador
53. Fundamedios – Equador
54. Garoa Hacker Clube – Brasilien
55. Global Partners Digital – Vereinigtes Königreich
56. GreenNet – Vereinigtes Königreich
57. GreatFire – China
58. Hiperderecho – Peru
59. Homo Digitalis – Griechenland
60. Human Rights in China – China
61. Human Rights Defenders Network – Sierra Leone
62. Human Rights Watch – International
63. Igarapé Institute -- Brasil
64. IFEX - International

65. Institute for Policy Research and Advocacy (ELSAM) – Indonesien

66. The Influencer Platform – Ukraine

67. INSM Network for Digital Rights – Irak

68. Internews Ukraine

69. Instituto Beta: Internet & Democracia (IBIDEM) – Brasilien

70. Instituto Brasileiro de Defesa do Consumidor (IDEC) – Brasilien

71. Instituto Educadigital – Brasilien

72. Instituto Nupef – Brasilien

73. Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec) – Brasilien

74. Instituto de Referência em Internet e Sociedade (IRIS) – Brasilien

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 – Dänemark

80. JCA-NET – Japan

81. KICTANet – Kenia

82. Korean Progressive Network Jinbonet – Südkorea

83. Laboratorio de Datos y Sociedad (Datysoc) – Uruguay

84. Laboratório de Políticas Públicas e Internet (LAPIN) – Brasilien

85. Latin American Network of Surveillance, Technology and Society Studies (LAVITS)

86. Lawyers Hub Afrika

87. Legal Initiatives for Vietnam

88. Ligue des droits de l'Homme (LDH) – Frankreich

89. Masaar - Technology and Law Community – Ägypten

90. Manushya Foundation – Thailand

91. MINBYUN Lawyers for a Democratic Society - Korea

92. Open Culture Foundation – Taiwan

93. Open Media – Kanada

94. Open Net Association – Korea

95. OpenNet Africa – Uganda

96. Panoptykon Foundation – Polen

97. Paradigm Initiative – Nigeria

98. Privacy International – International

99. Radio Viva – Paraguay

100. Red en Defensa de los Derechos Digitales (R3D) – Mexiko

101. Regional Center for Rights and Liberties – Ägypten

102. Research ICT Africa

103. Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC) – Kanada

104. Share Foundation - Serbien

105. Social Media Exchange (SMEX) – Libanon, Arabischer Raum

106. SocialTIC – Mexiko

107. Southeast Asia Freedom of Expression Network (SAFEnet) – Südostasien

108. Supporters for the Health and Rights of Workers in the Semiconductor Industry (SHARPS) – Südkorea

109. Surveillance Technology Oversight Project (STOP) – USA

110. Tecnología, Investigación y Comunidad (TEDIC) – Paraguay

111. Thai Netizen Network – Thailand

112. Unwanted Witness – Uganda

113. Vrijschrift – Niederlande

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 – Arabischer Raum

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

*Liste unterzeichnender Personen seit dem 13. Januar 2022