December 22, 2021

H.E. Ms. Faouzia Boumaiza Mebarki

Chairperson

Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes

Your Excellency,

We, the undersigned organizations and academics, work to protect and advance human rights, online and offline. Efforts to address cybercrime are of concern to us, both because cybercrime poses a threat to human rights and livelihoods, and because cybercrime laws, policies, and initiatives are currently being used to undermine people's rights. We therefore ask that the process through which the Ad Hoc Committee does its work includes robust civil society participation throughout all stages of the development and drafting of a convention, and that any proposed convention include human rights safeguards applicable to both its substantive and procedural provisions.

Background

The proposal to elaborate a comprehensive "international convention on countering the use of information and communications technologies for criminal purposes" is being put forward at the same time that UN human rights mechanisms are raising alarms about the abuse of cybercrime laws around the world. In his 2019 report, the UN special rapporteur on the rights to freedom of peaceful assembly and of association, Clément Nyaletsossi Voule, observed, "A surge in legislation and policies aimed at combating cybercrime has also opened the door to punishing and surveilling activists and protesters in many countries around the world." In 2019 and once again this year, the UN General Assembly expressed grave concerns that cybercrime legislation is being misused to target human rights defenders or hinder their work and endanger their safety in a manner contrary to international law. This follows years of reporting from non-governmental organizations on the human rights abuses stemming from overbroad cybercrime laws.

When the convention was first proposed, over 40 leading digital rights and human rights organizations and experts, including many signatories of this letter, urged delegations to vote against the resolution, warning that the proposed convention poses a threat to human rights.

In advance of the first session of the Ad Hoc Committee, we reiterate these concerns. If a UN convention on cybercrime is to proceed, the goal should be to combat the use of information and communications technologies for criminal purposes without endangering the fundamental rights of those it seeks to protect, so people can freely enjoy and exercise their rights, online and offline. Any proposed convention should incorporate clear and robust human rights safeguards. A convention without such safeguards or that dilutes States' human rights obligations would place individuals at risk and make our digital presence even more insecure, each threatening fundamental human rights.

As the Ad Hoc Committee commences its work drafting the convention in the coming months, it is vitally important to apply a human rights-based approach to ensure that the proposed text is not used as a tool to stifle freedom of expression, infringe on privacy and data protection, or endanger individuals and communities at risk.

The important work of combating cybercrime should be consistent with States' human rights obligations set forth in the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), and other international human rights instruments and standards. In other words, efforts to combat cybercrime should also protect, not undermine, human rights. We remind States that the same rights that individuals have offline should also be protected online.

Scope of Substantive Criminal Provisions

There is no consensus on how to tackle cybercrime at the global level or a common understanding or definition of what constitutes cybercrime. From a human rights perspective, it is essential to keep the scope of any convention on cybercrime narrow. Just because a crime might involve technology does not mean it needs to be included in the proposed convention. For example, expansive cybercrime laws often simply add penalties due to the use of a computer or device in the commission of an existing offense. The laws are especially problematic when they include content-related crimes. Vaguely worded cybercrime laws purporting to combat misinformation and online support for or glorification of terrorism and extremism, can be misused to imprison bloggers or block entire platforms in a given country. As such, they fail to comply with international freedom of expression standards. Such laws put journalists, activists, researchers, LGBTQ communities, and dissenters in danger, and can have a chilling effect on society more broadly.

Even laws that focus more narrowly on cyber-enabled crimes are used to undermine rights. Laws criminalizing unauthorized access to computer networks or systems have been used to target digital security researchers, whistleblowers, activists, and journalists. Too often, security researchers, who help keep everyone safe, are caught up in vague cybercrime laws and face criminal charges for identifying flaws in security systems. Some States have also interpreted unauthorized access laws so broadly as to effectively criminalize any and all whistleblowing; under these interpretations, any disclosure of information in violation of a corporate or government policy could be treated as "cybercrime." Any potential convention should explicitly include a malicious intent standard, should not transform corporate or government computer use policies into criminal liability, should provide a clearly articulated and expansive public interest defense, and include clear provisions that allow security researchers to do their work without fear of prosecution.

Human Rights and Procedural Safeguards

Our private and personal information, once locked in a desk drawer, now resides on our digital devices and in the cloud. Police around the world are using an increasingly intrusive set of investigative tools to access digital evidence. Frequently, their investigations cross borders without proper safeguards and bypass the protections in mutual legal assistance treaties. In many contexts, no judicial oversight is involved, and the role of independent data

protection regulators is undermined. National laws, including cybercrime legislation, are often inadequate to protect against disproportionate or unnecessary surveillance.

Any potential convention should detail robust procedural and human rights safeguards that govern criminal investigations pursued under such a convention. It should ensure that any interference with the right to privacy complies with the principles of legality, necessity, and proportionality, including by requiring independent judicial authorization of surveillance measures. It should also not forbid States from adopting additional safeguards that limit law enforcement uses of personal data, as such a prohibition would undermine privacy and data protection. Any potential convention should also reaffirm the need for States to adopt and enforce “strong, robust and comprehensive privacy legislation, including on data privacy, that complies with international human rights law in terms of safeguards, oversight and remedies to effectively protect the right to privacy."

There is a real risk that, in an attempt to entice all States to sign a proposed UN cybercrime convention, bad human rights practices will be accommodated, resulting in a race to the bottom. Therefore, it is essential that any potential convention explicitly reinforces procedural safeguards to protect human rights and resists shortcuts around mutual assistance agreements.

Meaningful Participation

Going forward, we ask the Ad Hoc Committee to actively include civil society organizations in consultations—including those dealing with digital security and groups assisting vulnerable communities and individuals—which did not happen when this process began in 2019 or in the time since.

Accordingly, we request that the Committee:

● Accredit interested technological and academic experts and nongovernmental groups, including those with relevant expertise in human rights but that do not have consultative status with the Economic and Social Council of the UN, in a timely and transparent manner, and allow participating groups to register multiple representatives to accommodate the remote participation across different time zones.

● Ensure that modalities for participation recognize the diversity of non-governmental stakeholders, giving each stakeholder group adequate speaking time, since civil society, the private sector, and academia can have divergent views and interests.

● Ensure effective participation by accredited participants, including the opportunity to receive timely access to documents, provide interpretation services, speak at the Committee’s sessions (in-person and remotely), and submit written opinions and recommendations.

● Maintain an up-to-date, dedicated webpage with relevant information, such as practical information (details on accreditation, time/location, and remote participation), organizational documents (i.e., agendas, discussions documents, etc.), statements and other interventions

by States and other stakeholders, background documents, working documents and draft outputs, and meeting reports.

Countering cybercrime should not come at the expense of the fundamental rights and dignity of those whose lives this proposed Convention will touch. States should ensure that any proposed cybercrime convention is in line with their human rights obligations, and they should oppose any proposed convention that is inconsistent with those obligations.

We would be highly appreciative if you could kindly circulate the present letter to the Ad Hoc Committee Members and publish it on the website of the Ad Hoc Committee.

Signatories,*

Access Now – International
Alternative ASEAN Network on Burma (ALTSEAN) – Burma
Alternatives – Canada
Alternative Informatics Association – Turkey
AqualtuneLab – Brazil
ArmSec Foundation – Armenia
ARTICLE 19 – International
Asociación por los Derechos Civiles (ADC) – Argentina
Asociación Trinidad / Radio Viva – Trinidad
Asociatia Pentru Tehnologie si Internet (ApTI) – Romania
Association for Progressive Communications (APC) – International
Associação Mundial de Rádios Comunitárias (Amarc Brasil) – Brazil
ASEAN Parliamentarians for Human Rights (APHR) – Southeast Asia
Bangladesh NGOs Network for Radio and Communication (BNNRC) – Bangladesh
BlueLink Information Network – Bulgaria
Brazilian Institute of Public Law - Brazil
Cambodian Center for Human Rights (CCHR) – Cambodia
Cambodian Institute for Democracy – Cambodia
Cambodia Journalists Alliance Association – Cambodia
Casa de Cultura Digital de Porto Alegre – Brazil
Centre for Democracy and Rule of Law – Ukraine
Centre for Free Expression – Canada
Centre for Multilateral Affairs – Uganda
Center for Democracy & Technology – United States
Center for Justice and International Law (CEJIL) - International
Centro de Estudios en Libertad de Expresión y Acceso (CELE) – Argentina
Civil Society Europe
Coalition Direitos na Rede – Brazil
Código Sur - Costa Rica
Collaboration on International ICT Policy for East and Southern Africa (CIPESA) – Africa
CyberHUB-AM – Armenia
Data Privacy Brazil Research Association – Brazil
Dataskydd – Sweden
Derechos Digitales – Latin America
Defending Rights & Dissent – United States

Digital Citizens – Romania
DigitalReach – Southeast Asia
Digital Rights Watch - Australia
Digital Security Lab – Ukraine
Državljan D / Citizen D – Slovenia
Electronic Frontier Foundation (EFF) – International
Electronic Privacy Information Center (EPIC) – United States
Elektronisk Forpost Norge – Norway
Epicenter.works for digital rights – Austria
European Center For Not-For-Profit Law (ECNL) Stichting – Europe
European Civic Forum – Europe
European Digital Rights (EDRi) – Europe
eQuality Project – Canada
Fantsuam Foundation – Nigeria
Free Speech Coalition – United States
Foundation for Media Alternatives (FMA) – Philippines
Fundación Acceso – Central America
Fundación Ciudadanía y Desarrollo de Ecuador
Fundación CONSTRUIR – Bolivia
Fundacion Datos Protegidos – Chile
Fundación EsLaRed de Venezuela
Fundación Karisma – Colombia
Fundación OpenlabEC – Ecuador
Fundamedios – Ecuador
Garoa Hacker Clube – Brazil
Global Partners Digital – United Kingdom
GreenNet – United Kingdom
GreatFire – China
Hiperderecho – Peru
Homo Digitalis – Greece
Human Rights in China – China
Human Rights Defenders Network – Sierra Leone
Human Rights Watch – International
Igarapé Institute -- Brazil
IFEX - International
Institute for Policy Research and Advocacy (ELSAM) – Indonesia
The Influencer Platform – Ukraine
INSM Network for Digital Rights – Iraq
Internews Ukraine
InternetNZ – New Zealand
Instituto Beta: Internet & Democracia (IBIDEM) – Brazil
Instituto Brasileiro de Defesa do Consumidor (IDEC) – Brazil
Instituto Educadigital – Brazil
Instituto Nupef – Brazil
Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec) – Brazil
Instituto de Referência em Internet e Sociedade (IRIS) – Brazil
Instituto Panameño de Derecho y Nuevas Tecnologías (IPANDETEC) – Panama
Instituto para la Sociedad de la Información y la Cuarta Revolución Industrial – Peru

International Commission of Jurists – International
The International Federation for Human Rights (FIDH)
IT-Pol – Denmark
JCA-NET – Japan
KICTANet – Kenya
Korean Progressive Network Jinbonet – South Korea
Laboratorio de Datos y Sociedad (Datysoc) – Uruguay
Laboratório de Políticas Públicas e Internet (LAPIN) – Brazil
Latin American Network of Surveillance, Technology and Society Studies (LAVITS)
Lawyers Hub Africa
Legal Initiatives for Vietnam
Ligue des droits de l'Homme (LDH) – France
Masaar - Technology and Law Community – Egypt
Manushya Foundation – Thailand
MINBYUN Lawyers for a Democratic Society - Korea
Open Culture Foundation – Taiwan
Open Media – Canada
Open Net Association – Korea
OpenNet Africa – Uganda
Panoptykon Foundation – Poland
Paradigm Initiative – Nigeria
Privacy International – International
Radio Viva – Paraguay
Red en Defensa de los Derechos Digitales (R3D) – Mexico
Regional Center for Rights and Liberties – Egypt
Research ICT Africa
Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC) – Canada
Share Foundation - Serbia
Social Media Exchange (SMEX) – Lebanon, Arab Region
SocialTIC – Mexico
Southeast Asia Freedom of Expression Network (SAFEnet) – Southeast Asia
Supporters for the Health and Rights of Workers in the Semiconductor Industry (SHARPS) – South Korea
Surveillance Technology Oversight Project (STOP) – United States
Tecnología, Investigación y Comunidad (TEDIC) – Paraguay
Thai Netizen Network – Thailand
Unwanted Witness – Uganda
Vrijschrift – Netherlands
West African Human Rights Defenders Network – Togo
World Movement for Democracy – International
7amleh – The Arab Center for the Advancement of Social Media – Arab Region

Individual Experts and Academics

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

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

*List of signatories as of February 25, 2022