

Declaración conjunta de la sociedad civil: Los Estados deben respetar los derechos humanos al emplear tecnologías de vigilancia digital para combatir la pandemia

2 de abril de 2020

La pandemia de COVID-19 es una emergencia global de salud pública, que precisa de una respuesta coordinada y en gran escala de los gobiernos en todo el mundo. Sin embargo, las iniciativas de los Estados para contener el virus no deben servir para encubrir el inicio de una nueva era marcada por una enorme expansión de los sistemas de vigilancia digital invasiva.

Las organizaciones abajo firmantes instamos a los gobiernos a dar muestra de liderazgo en la gestión de la pandemia garantizando que el empleo de tecnologías digitales para rastrear y monitorear a personas y poblaciones respeta plenamente los derechos humanos.

La tecnología puede y debe desempeñar importantes funciones durante este esfuerzo que se está realizando para salvar vidas, como difundir mensajes de salud pública y aumentar el acceso a los servicios de salud. No obstante, el aumento de los poderes de vigilancia digital de los Estados –como tener acceso a los datos de localización de los teléfonos móviles– amenaza la privacidad, la libertad de expresión y la libertad de asociación de una manera que podría violar derechos y reducir la confianza en las autoridades públicas, con el consiguiente menoscabo de la eficacia de las repuestas de salud pública. Tales medidas entrañan también un riesgo de discriminación y pueden perjudicar de manera desproporcionada a comunidades ya marginadas.

Vivimos tiempos extraordinarios, pero el derecho de los derechos humanos sigue siendo aplicable. De hecho, el marco de los derechos humanos tiene por objeto garantizar un cuidadoso equilibrio de los distintos derechos para proteger a las personas y las sociedades en general. Los Estados no pueden desatender sin más derechos como la privacidad y la libertad de expresión con el pretexto de gestionar una crisis de salud pública. Al contrario, la protección de los derechos humanos también promueve la salud pública. Ahora más que nunca, los gobiernos deben garantizar estrictamente que toda restricción de estos derechos se ajusta a las salvaguardias de los derechos humanos ya establecidas.

Esta crisis nos brinda la oportunidad de demostrar la humanidad que compartimos. Para combatir esta pandemia, podemos hacer esfuerzos extraordinarios que sean compatibles con las normas de derechos humanos y el Estado de derecho. Las decisiones que los gobiernos tomen ahora para afrontar la pandemia determinarán cómo será el mundo en el futuro.

Pedimos a todos los gobiernos que no respondan a la pandemia de COVID-19 incrementando la vigilancia digital si no se cumplen las condiciones siguientes:

1. Las medidas de vigilancia adoptadas para abordar la pandemia deben ser legales, necesarias y proporcionadas. Han de estar previstas por la ley y justificadas por objetivos legítimos de salud pública, determinados por las autoridades de salud pública competentes, y ser proporcionadas a esas necesidades. Los gobiernos deben ser transparentes con respecto a las medidas que tomen, para que puedan ser analizadas y modificadas, retiradas o anuladas posteriormente, si procede. No podemos dejar que la pandemia de COVID-19 sirva de excusa para ejercer vigilancia masiva indiscriminada.
2. Si los gobiernos amplían los poderes de seguimiento y vigilancia, tales poderes han de ser de duración limitada y prolongarse sólo durante el tiempo necesario para abordar la pandemia actual. No podemos dejar que la pandemia de COVID-19 sirva de excusa para ejercer vigilancia indefinidamente.

3. Los Estados deben garantizar que el aumento de la recopilación, conservación y agregación de datos personales, incluidos los relativos a la salud, tiene como único fin responder a la pandemia de COVID-19. Los datos recopilados, conservados y agregados para responder a la pandemia deben tener un alcance y duración limitados en función de la pandemia y no utilizarse con fines comerciales ni de otra índole. No podemos dejar que la pandemia de COVID-19 sirva de excusa para menoscabar el derecho personal a la privacidad.

4. Los gobiernos deben hacer todo lo posible para proteger los datos personales, lo que incluye garantizar la debida seguridad de los datos recopilados y de los dispositivos, aplicaciones, redes o servicios utilizados en su recopilación, transmisión, tratamiento y almacenamiento. Cuando se afirme que los datos son anónimos, ha de poder demostrarse y respaldarse con información suficiente sobre cómo se han anonimizado. No podemos dejar que los intentos de responder a esta pandemia sirvan de justificación para poner en riesgo la seguridad digital de las personas.

5. Todo uso de tecnologías de vigilancia digital en la respuesta a la COVID-19, incluidos los sistemas de inteligencia de datos y artificial, debe tener en cuenta el riesgo de que tales herramientas faciliten la discriminación y otros abusos contra los derechos de las minorías raciales, las personas que viven en la pobreza y las poblaciones marginadas, cuyas necesidades y realidades de vida pueden quedar ocultas o mal representadas en los macroconjuntos de datos. No podemos dejar que la pandemia de COVID-19 aumente aún más las diferencias existentes en el disfrute de los derechos humanos entre distintos grupos de la sociedad.

6. Si los gobiernos firman acuerdos para compartir datos con otras entidades públicas o del sector privado, deben hacerlo basándose en la ley, y la existencia de tales acuerdos, así como la información necesaria para evaluar su impacto en la privacidad y los derechos humanos, debe revelarse públicamente, por escrito, con las cláusulas de suspensión y con supervisión pública y otras salvaguardias por defecto. Las empresas participantes en las iniciativas de los gobiernos frente a la COVID-19 deben ejercer la diligencia debida para garantizar que respetan los derechos humanos y que toda intervención está desligada de otros intereses empresariales y comerciales. No podemos dejar que la pandemia de COVID-19 sirva de excusa para ocultar a la sociedad qué información recopila y comparte con terceros su gobierno.

7. Toda respuesta debe incorporar mecanismos de rendición de cuentas y salvaguardias contra el uso indebido. El aumento de las medidas de vigilancia ante la COVID-19 no debe ser competencia de los organismos de seguridad o inteligencia, y tiene que estar sujeto a la supervisión efectiva de órganos independientes adecuados. Además, se debe ofrecer a las personas la oportunidad de conocer e impugnar toda medida que se tome en relación con la COVID-19 para recopilar, agregar, conservar y emplear datos. Las personas que hayan sido sometidas a vigilancia han de tener acceso a medios efectivos para interponer recursos.

8. Las respuestas a la COVID-19 que contengan medidas de recopilación de datos han de incluir medios de participación libre, activa y significativa de las partes interesadas pertinentes, en particular de especialistas del sector de la salud pública y de los grupos de población más marginados.

Organizaciones firmantes:

7amleh – Arab Center for Social Media Advancement

Access Now

African Declaration on Internet Rights and Freedoms Coalition

AI Now

Algorithm Watch

Alternatif Bilisim

Amnistía Internacional

ApTI
ARTICLE 19
Asociación para una Ciudadanía Participativa, ACI Participa
Association for Progressive Communications (APC)
ASUTIC, Senegal
Athán - Freedom of Expression Activist Organization
Australian Privacy Foundation
Barracón Digital
Big Brother Watch
Bits of Freedom
Center for Advancement of Rights and Democracy (CARD)
Center for Digital Democracy
Center for Economic Justice
Centro De Estudios Constitucionales y de Derechos Humanos de Rosario
Chaos Computer Club - CCC
Citizen D / Državljan D
CIVICUS
Civil Liberties Union for Europe
CódigoSur
Coding Rights
Coletivo Brasil de Comunicação Social
Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
Comité por la Libre Expresión (C-Libre)
Committee to Protect Journalists
Consumer Action
Consumer Federation of America
Cooperativa Tierra Común
Creative Commons Uruguay
D3 - Defesa dos Direitos Digitais
Data Privacy Brasil
Democratic Transition and Human Rights Support Center "DAAM"
Derechos Digitales
Digital Rights Lawyers Initiative (DRLI)
Digital Rights Watch
Digital Security Lab Ukraine
Digitalcourage
EPIC
epicenter.works
European Digital Rights - EDRI
Fitug
Foundation for Information Policy Research
Foundation for Media Alternatives
Fundación Acceso (Centroamérica)
Fundación Ciudadanía y Desarrollo, Ecuador
Fundación Datos Protegidos
Fundación Internet Bolivia
Fundación Taigüey, República Dominicana
Fundación Vía Libre
Hermes Center

Hiperderecho
Homo Digitalis
Human Rights Watch
Hungarian Civil Liberties Union
ImpACT International for Human Rights Policies
Index on Censorship
Initiative für Netzfreiheit
Innovation for Change - Middle East and North Africa
International Commission of Jurists
International Service for Human Rights (ISHR)
Intervozes - Coletivo Brasil de Comunicação Social
Ipandetec
IPPF
Irish Council for Civil Liberties (ICCL)
IT-Political Association of Denmark
Iuridicum Remedium z.s. (IURE)
Karisma
La Quadrature du Net
Liberia Information Technology Student Union
Liberty
Luchadoras
Majal.org
Masaar "Community for Technology and Law"
Media Rights Agenda (Nigeria)
MENA Rights Group
Metamorphosis Foundation
New America's Open Technology Institute
Observacom
Open Data Institute
Open Rights Group
OpenMedia
OutRight Action International
Pangea
Panoptikon Foundation
Paradigm Initiative (PIN)
PEN International
Privacy International
Public Citizen
Public Knowledge
R3D: Red en Defensa de los Derechos Digitales
RedesAyuda
SHARE Foundation
Skyline International for Human Rights
Sursiendo
Swedish Consumers' Association
Tahrir Institute for Middle East Policy (TIMEP)
Tech Inquiry
TechHerNG
TEDIC

The Bachchao Project
Unwanted Witness, Uganda
Usuarios Digitales
WITNESS
World Wide Web Foundation