

Declaração conjunta da sociedade civil: A utilização de tecnologias de vigilância digital pelos Estados para combater a pandemia deve respeitar os direitos humanos

2 de Abril de 2020

A pandemia COVID-19 é uma emergência de saúde pública global que requer uma resposta coordenada e em larga escala pelos governos de todo o mundo. No entanto, os esforços dos Estados para conter o vírus não devem ser utilizados como cobertura para nova era de ampla expansão de sistemas de vigilância digital invasiva.

Nós, as organizações abaixo-assinadas, exortamos os governos a mostrar liderança no combate à pandemia de uma forma que assegure que a utilização de tecnologias digitais para localizar e monitorizar indivíduos e populações seja feita com estrito respeito pelos direitos humanos.

A tecnologia pode e deve desempenhar um papel importante durante este esforço para salvar vidas, por exemplo, para disseminar mensagens de saúde pública e aumentar o acesso aos cuidados de saúde. No entanto, um aumento dos poderes de vigilância digital estatais, tais como obter acesso aos dados de localização dos telemóveis, ameaça a privacidade, a liberdade de expressão e a liberdade de associação de formas que podem violar direitos e degradar a confiança nas autoridades públicas - prejudicando a eficácia de qualquer resposta em matéria de saúde pública. Tais medidas representam igualmente um risco de discriminação e podem prejudicar de forma desproporcionada comunidades já marginalizadas.

Estes são tempos extraordinários, mas os direitos humanos ainda vigoram. De facto, o quadro legal dos direitos humanos foi concebido de forma a assegurar que os diferentes direitos possam ser cuidadosamente ponderados para proteger os indivíduos e as sociedades em geral. Os Estados não podem simplesmente desrespeitar direitos como a privacidade e a liberdade de expressão, em nome da resolução de uma crise de saúde pública. Pelo contrário, a protecção dos direitos humanos também promove a saúde pública. Agora, mais do que nunca, os governos devem rigorosamente assegurar que quaisquer restrições a estes direitos estão em conformidade com as salvaguardas há muito estabelecidas em matéria de direitos humanos.

Esta crise constitui uma oportunidade para demonstrar a nossa humanidade comum. Podemos fazer esforços extraordinários para combater esta pandemia que sejam coerentes com as normas de direitos humanos e com o Estado de direito. As decisões que os governos agora tomam para fazer face à pandemia irão moldar o aspecto do mundo no futuro.

Exortamos todos os governos a não responderem à pandemia da COVID-19 com uma vigilância digital acrescida, salvo estando reunidas as seguintes condições:

1. As medidas de vigilância adoptadas para fazer face à pandemia devem ser lícitas, necessárias e proporcionais. Devem ser previstas por lei e justificadas por objectivos legítimos de saúde pública, tal como determinado pelas devidas autoridades de saúde pública, e serem proporcionais a essas necessidades. Os governos devem ser transparentes sobre as medidas que estão a tomar para que possam ser escrutinadas e, se for caso disso, posteriormente modificadas, revogadas ou anuladas. Não podemos permitir que a pandemia da COVID-19 sirva de desculpa para uma vigilância massiva e indiscriminada.

2. Se os governos alargarem os poderes de controlo e vigilância, esses poderes devem ser limitados no tempo, e apenas durarem o tempo necessário para fazer face à actual pandemia. Não podemos permitir que a pandemia COVID-19 sirva de desculpa para uma vigilância que não tenha o seu fim definido no tempo.
3. Os Estados devem assegurar que uma maior recolha, retenção e agregação de dados pessoais, incluindo dados de saúde só é utilizada para efeitos de resposta à pandemia da COVID-19. Os dados recolhidos, retidos, e agregados para responder à pandemia devem ser limitados no seu âmbito, limitados no tempo tendo por referência a pandemia e não devem ser utilizados para fins comerciais ou quaisquer outros. Não podemos permitir que a pandemia da COVID-19 sirva de pretexto para esvaziar o direito individual à privacidade.
4. Os governos devem envidar todos os esforços para proteger os dados das pessoas, incluindo garantir segurança suficiente de quaisquer dados pessoais recolhidos e de quaisquer dispositivos, aplicações, redes ou serviços envolvidos na recolha, transmissão, processamento e armazenamento desses dados. Quaisquer alegações de que os dados são anónimos devem ser baseadas em provas e suportadas em informação suficiente sobre a forma como foi realizada a anonimização. Não podemos permitir que tentativas de resposta a esta pandemia sejam usadas como justificação para comprometer a segurança digital das pessoas.
5. Qualquer uso de tecnologias de vigilância digital em resposta à COVID-19, incluindo *big data* e sistemas de inteligência artificial, deve levar em conta o risco de estes instrumentos facilitarem a discriminação e outros abusos contra os direitos de minorias raciais, pessoas que vivem na pobreza e outras populações marginalizadas, cujas necessidades e realidades podem ser ocultadas ou deturpadas em grandes conjuntos de dados. Não podemos permitir que a pandemia COVID-19 aumente ainda mais o fosso na fruição dos direitos humanos entre os diferentes grupos da sociedade.
6. Se os governos celebrarem acordos de partilha de dados com outras entidades do sector público ou privado, estes devem ser feitos com base na lei, e a existência destes acordos e das informações necessárias à avaliação do seu impacto no direito à privacidade e nos direitos humanos devem ser publicamente divulgados - por escrito, com cláusulas de caducidade, supervisão pública e outras salvaguardas por defeito. As empresas envolvidas em esforços dos governamentais para combater a COVID-19 devem empreender as devidas diligências para garantir que respeitam os direitos humanos, e assegurar que qualquer intervenção se encontre blindada contra outros interesses empresariais e comerciais. Não podemos permitir que a pandemia da COVID-19 sirva de desculpa para ocultar das pessoas que informações estão os governos a recolher e a partilhar com terceiros.
7. Qualquer resposta deve incorporar protecções e salvaguardas de responsabilização contra abusos. Acrescidos esforços de vigilância relacionados com a COVID-19 não cair na esfera dos serviços de informações de segurança e devem estar sujeitas a uma supervisão efectiva por parte dos respectivos órgãos de supervisão independentes. Além disso, às pessoas individualmente consideradas deve ser dada a oportunidade de conhecer e contestar

quaisquer medidas relacionadas com a COVID-19 que tenham por fim recolher, agregar, reter e utilizar dados. Quem tenha sido sujeito a vigilância deve ter acesso a meios de reparação eficazes.

8. Respostas relacionadas com a COVID-19 que incluam esforços de recolha de dados devem incluir os meios que permitam uma participação gratuita, activa e significativa das partes interessadas, em especial peritos do sector da saúde pública e de grupos populacionais mais marginalizados.

Signatários:

7amleh – Arab Center for Social Media Advancement
Access Now
African Declaration on Internet Rights and Freedoms Coalition
AI Now
Algorithm Watch
Alternatif Bilisim
Amnesty International
ApTI
ARTICLE 19
Asociación para una Ciudadanía Participativa, ACI Participa
Association for Progressive Communications (APC)
ASUTIC, Senegal
Athar - 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
Ipanetec
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