European Center for Not-for-Profit Law

INCLO
INTERNATIONAL NETWORK OF CIVIL LIBERTIES ORGANIZATIONS

PRIVACY INTERNATIONAL

Bajo control: el (ab)uso de tecnologías de vigilancia en las respuestas estatales al Covid-19

Lecciones mundiales de la pandemia

Índice

Introducción....4

Antecedentes del proyecto....4
Alcance del proyecto....5
Metodología....8

Tendencias principales....10

TENDENCIA NRO. 1

La adaptación de las medidas de seguridad existentes a nuevos fines

Los críticos del gobierno en el blanco de las leyes sobre ciberdelincuencia adaptadas a nuevos fines....11

Caso de Kenia: Criminalización de la disidencia bajo el pretexto de luchar contra la desinformación sobre el Covid-19....13

Más facultades para los servicios de inteligencia....14

TENDENCIA NRO. 2

El silenciamiento de la sociedad civil

El efecto disuasorio de las sanciones penales....18

Espacios públicos bajo vigilancia....19

Caso de Francia: Vigilancia ilegal con drones....21

TENDENCIA NRO. 3

El riesgo del uso indebido de datos personales

Intromisiones ilegales en la privacidad: Falta de claridad con respecto los fines de las aplicaciones relacionadas con el Covid-19 y las garantías aplicables....22

Caso de Indonesia: Las malas prácticas de almacenamiento de datos dejan desprotegidos a los datos personales de los usuarios....23

Preocupaciones relativas al Estado de Derecho....24

Predicciones erróneas y pocas vías de reparación....24

Caso de Colombia: Falta de transparencia de la aplicación de rastreo de contactos....25

TENDENCIA NRO. 4

El influyente papel de las empresas privadas

Colaboraciones poco claras entre los sectores público y privado....27

La influencia del sector privado en el establecimiento de normas universales en situaciones de crisis....28

Caso de Sudáfrica: Preocupación por la privacidad debido a la excesiva dependencia de WhatsApp....29

TENDENCIA NRO. 5

La normalización de la vigilancia más allá de la pandemia

La adaptación de las aplicaciones de Covid-19 a nuevos fines....32

El uso indebido de los datos recogidos con fines sanitarios de urgencia....34

Caso de la India: Polémicas en torno a la nueva finalidad de la app de rastreo de contactos y su impacto en el derecho a la privacidad....35

Acciones de la sociedad civil contra las medidas de vigilancia que resultaron exitosas....36

La lucha contra los drones en Francia....37
La defensa de las libertades fundamentales en Colombia....38
La resistencia a la vigilancia masiva en Israel....40

Conclusión....42

Recomendaciones....48

Recomendaciones detalladas....50

Para los agentes estatales....50
Para las empresas....53
Para la sociedad civil....54

Quiénes somos....55

Introducción

Antecedentes del proyecto

En los meses posteriores a la declaración de emergencia de salud pública por parte de la Organización Mundial de la Salud el 30 de enero de 2020, más de la mitad de los países del mundo adoptaron medidas de emergencia en respuesta a la pandemia de Covid-19. Junto con estas medidas de emergencia, se produjo **un incremento de los poderes del Ejecutivo, la suspensión del Estado de derecho y el recrudecimiento de los protocolos de seguridad**, con las consiguientes consecuencias sobre los derechos humanos fundamentales, como las libertades de expresión, reunión, asociación, información, privacidad y circulación, entre otras. Según el Secretario General de la ONU, António Guterres, **algunos gobiernos utilizaron la pandemia como pretexto para promover sus propios objetivos políticos**, introduciendo medidas de seguridad de emergencia para "aplastar la disidencia, criminalizar el ejercicio de libertades básicas, silenciar a las fuentes de información independiente y restringir las actividades de las organizaciones no gubernamentales". El impacto de estas medidas de emergencia en el espacio cívico ha sido ya bien documentado por los procedimientos especiales de la ONU, los organismos multilaterales regionales, los defensores de los derechos humanos y las organizaciones de la sociedad civil.

En este contexto de reducción del espacio cívico como consecuencia de las medidas de emergencia, se ha producido **un aumento rápido y sin precedentes del uso de tecnologías que permiten una vigilancia generalizada por parte de los gobiernos**. Estas tecnologías incluyen aplicaciones de rastreo de contactos y control de cuarentenas, vigilancia con drones, rastreo de tarjetas SIM, pulseras electrónicas, tecnologías biométricas (como las de reconocimiento facial), y extracción de datos de las redes sociales en busca de referencias al Covid-19. En algunos casos, las tecnologías se desplegaron con medidas normativas que criminalizan el incumplimiento de los protocolos de Covid-19. Las tecnologías de vigilancia se utilizaron en la fase de detección para identificar a las personas que, supuestamente, habían infringido la cuarentena o difundido información errónea sobre el virus; estas personas fueron como consecuencia sancionadas bajo el paraguas de las medidas legales de emergencia. Como se detalla en este informe, muchas de estas tecnologías se desarrollaron e implementaron de forma poco transparente, sin los marcos jurídicos apropiados ni mecanismos de rendición de cuentas y supervisión, y sin cláusulas de caducidad que estipularan claramente cuándo se irían dejando de utilizar.

Las tecnologías de vigilancia exacerbaron el impacto de las medidas de emergencia tomadas en relación con el Covid-19 en el espacio cívico, ya que permitieron a los gobiernos recopilar datos muy específicos sobre las personas mientras trabajaban con grandes cantidades de información, de una forma sin precedente en la historia de las pandemias mundiales. Consideramos a estas tecnologías como **facilitadoras**, ya que permitieron a los Estados implementar medidas de emergencia, tales como el distanciamiento social y el confinamiento obligatorio (en algunos casos, en detrimento de la libertad de reunión) y **aceleradoras**, ya que hicieron que las respuestas de emergencia fueran más eficientes y, a la vez, más intrusivas (al infringir, por ejemplo, el derecho a la privacidad). Como se muestra en este informe, estas tecnologías tan poderosas y cada vez más omnipresentes tuvieron, y siguen teniendo, serias consecuencias para el goce de los derechos humanos, y para la sociedad civil en general.

Alcance del proyecto

Con el objetivo de luchar contra el creciente autoritarismo, la Emergency Powers Coalition, un colectivo de organizaciones de la sociedad civil de todo el mundo, ha estado trabajando para resistir y ponerle fin a las medidas adoptadas extraordinariamente en las regulaciones nacionales y reforzar los estándares internacionales en la materia. Como parte de este esfuerzo, el European Center for Not-for-Profit Law (ECNL), la International Network of Civil Liberties Organizations (INCLO) y Privacy International (PI) se unieron para investigar el impacto negativo que tuvieron el uso de tecnologías de vigilancia y las medidas empleadas durante la pandemia de Covid-19 en los movimientos y organizaciones sociales. En este informe se ofrecen las principales conclusiones de esta investigación y se brindan recomendaciones para asegurar que las respuestas tecnológicas en futuras emergencias se desplieguen con un enfoque basado en derechos humanos.

Introducción

Realizamos un amplio estudio de las medidas de vigilancia de Covid-19 adoptadas en **15 países en los que trabajan las organizaciones miembro de INCLO** y, con la ayuda de aliados que realizaron investigaciones en el terreno, nos concentramos **en seis de ellos** (Colombia, Francia, India, Indonesia, Kenia y Sudáfrica), y utilizamos los ejemplos más representativos de estos países sobre las medidas adoptadas durante la pandemia. Si bien nuestros estudios de casos se centraron en estos seis países, las medidas de vigilancia de Covid-19 tienen, en realidad, un impacto a nivel mundial. Encontramos pruebas de su uso en todo el mundo, desde las democracias hasta los estados más autoritarios, en los seis casos estudiados.

Al realizar la investigación para este informe, intentamos comprender qué ocurrió realmente tras la implementación de las medidas de vigilancia, más allá de la oleada inicial de cobertura mediática. Investigamos las siguientes cuestiones, teniendo en cuenta otras medidas más amplias que fueron tomadas en relación con el Covid-19, el contexto político y el espacio cívico en los países seleccionados:

1. ¿Qué sucedió desde que se introdujeron por primera vez las medidas de vigilancia?
2. ¿Cuáles fueron sus impactos?
3. ¿Cómo se vieron afectados los distintos grupos de la sociedad? ¿Hay grupos demográficos más afectados que otros?
4. ¿Siguen vigentes las medidas de vigilancia o fueron derogadas/anuladas?
5. ¿Hubo resistencia, litigios o acciones de incidencia en respuesta a la vigilancia relacionada con la pandemia? ¿Qué podemos aprender de estas acciones?

Hemos identificado las siguientes cinco **tendencias generales:**

1. La reutilización de las medidas de seguridad y vigilancia preexistentes.
2. El silenciamiento de la sociedad civil.
3. El riesgo de uso indebido de los datos personales.
4. El influyente papel de las empresas privadas.
5. La normalización de la vigilancia más allá de la pandemia.

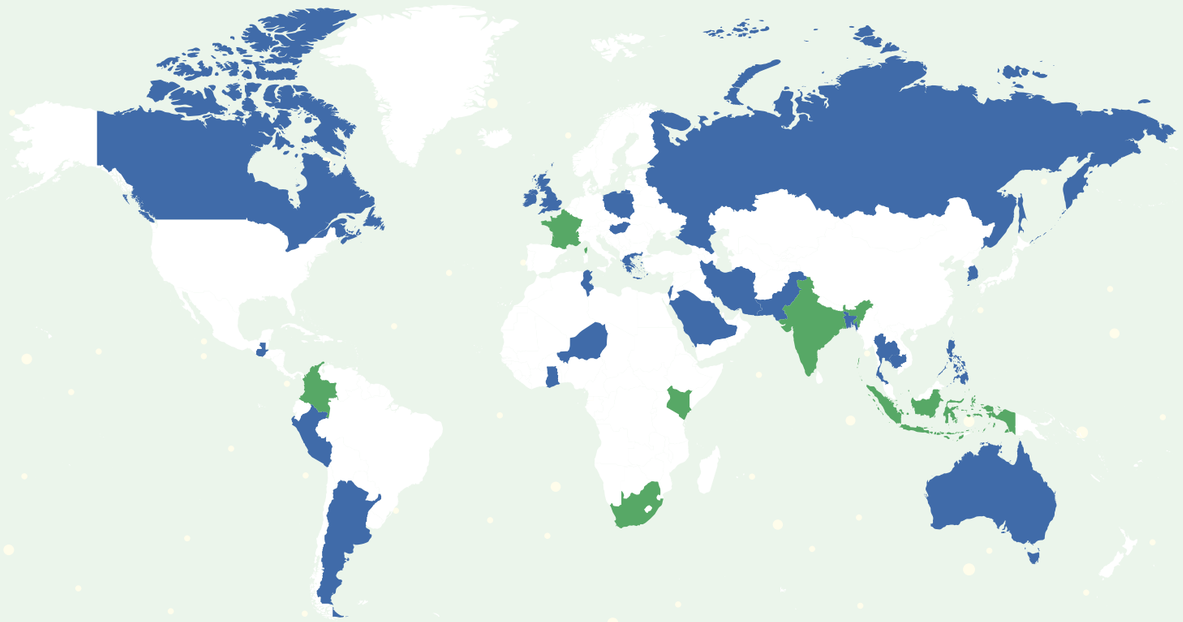


Imagen 1. El mapa muestra, en verde, los países en los que realizamos estudios de casos en profundidad y, en azul, los países mencionados en el informe.

En este informe, profundizamos en cada una de estas cuestiones, brindamos ejemplos ilustrativos y analizamos las amenazas para los derechos humanos, incluidas la libertad de asociación y reunión, el derecho a la privacidad y la libertad de circulación. Reconocemos que este ejercicio de mapeo no refleja todas las posibles consecuencias de las medidas de vigilancia adoptadas durante la pandemia. No obstante, esperamos que aporte una perspectiva desde la sociedad civil que resulte valiosa para el debate sobre las respuestas tecnológicas a futuras emergencias y la indispensable protección de los derechos humanos.

Reconocemos que la pandemia de Covid-19 aún está en curso y que los países se encuentran en diferentes fases del camino hacia la recuperación. Los casos y análisis presentados en este informe se refieren a un periodo específico de la pandemia: de enero de 2020 a octubre de 2022. Aunque muchas de las medidas de vigilancia implementadas al principio de la pandemia ya se han suspendido, la situación requerirá un seguimiento continuo antes de que podamos comprender el impacto a largo plazo sobre la sociedad civil.

Metodología

- La metodología de este estudio incluyó:
- La investigación documental y el análisis de documentos políticos, informes de los medios de comunicación y libros blancos.
- El envío de una encuesta a las organizaciones miembros de la INCLO, que representan a la sociedad civil en 15 países.
- Las investigaciones locales realizadas por organizaciones aliadas en Colombia, Francia, India, Indonesia, Kenia y Sudáfrica.
- La síntesis y el análisis de los informes presentados por las organizaciones aliadas.
- El debate de las principales conclusiones y tendencias en los distintos países durante las reuniones del equipo internacional del proyecto.

Tendencia nro. 1: La adaptación de las medidas de seguridad existentes a nuevos fines

Con el fin de implementar rápidamente medidas de vigilancia relacionadas con el Covid-19, **algunos gobiernos aprovecharon las estructuras y los recursos existentes que se habían desplegado originalmente para la lucha contra el terrorismo**. A modo de ejemplo, hicieron uso de la legislación antiterrorista vigente, de los servicios de inteligencia nacionales, desplegaron tecnologías militares, etc. Este tipo de "adaptación" fue fomentada por el sector privado. Una investigación de *Reuters* identificó "al menos ocho empresas de vigilancia y ciberinteligencia que intentaban venderle **herramientas de espionaje y orden público con una nueva finalidad**" a los gobiernos, para lo cual cambiaron la descripción de sus productos a herramientas para rastrear el virus y hacer cumplir cuarentenas. Observamos una tendencia general en la que las leyes, tecnologías y agencias que, anteriormente, estaban asociadas con la lucha antiterrorista y la seguridad nacional fueron redireccionadas hacia el nuevo objetivo de luchar contra la propagación del Covid-19.[1]

El uso de las leyes de ciberdelincuencia contra los críticos al gobierno

Las leyes sobre ciberdelincuencia se utilizaron durante la pandemia para justificar la vigilancia de la actividad en internet y de la difusión de información sobre el virus. Por ejemplo, el gobierno de Níger reutilizó su Ley de Ciberdelincuencia de 2019 y el periodista Mamane Kaka Touda fue detenido y encarcelado bajo el cargo de "difusión de datos con la intención de alterar el orden público" debido a una publicación en las redes sociales sobre un presunto caso de Covid-19. Del mismo modo, en Arabia Saudí, el gobierno anunció que "los mensajes en las redes sociales que cuestionen el toque de queda por COVID-19 o se manifiesten en su contra" serían objeto de enjuiciamiento en virtud de la Ley contra la Ciberdelincuencia. Freedom House informó que, en

[1] Para más detalles, véase el informe de la Relatora Especial de la ONU sobre la lucha contra el terrorismo y los derechos humanos, Fionnuala Ni Aolain, *Covid-19, Counter-terrorism and Emergency Law.*

2020, un hombre saudí fue detenido por compartir "noticias de fuentes desconocidas" sobre Covid-19. Según el informe, se enfrentaba a una pena de cinco años de prisión y a una multa de 800.000 dólares en virtud de la Ley contra la Ciberdelincuencia. También se invocaron leyes sobre ciberdelincuencia contra ciudadanos de Bangladesh y Kenia que, supuestamente, habían difundido información errónea sobre el Covid-19.

En algunos casos, **los gobiernos reutilizaron las leyes sobre ciberdelincuencia para imponer (o amenazar con imponer) penas desproporcionadas y atacar a los críticos del gobierno**. En Indonesia, el Ministerio de Comunicación e Información anunció su intención de tomar fuertes medidas contra los "engaños" relacionados con el Covid-19, amenazando a los infractores con penas de hasta seis años de prisión o una multa máxima de 1.000 millones de rupias (más de 60.000 dólares estadounidenses), según lo establecido en la Ley sobre Información y Transacciones Electrónicas (ley ITE). Asimismo, en febrero de 2021, el gobierno indonesio amplió la ley ITE con la creación de una Unidad de Policía Virtual, para adelantarse a los "posibles ciberdelitos" y prevenirlos mediante la vigilancia de los contenidos de las redes sociales. En la práctica, la **Policía Virtual envió advertencias a usuarios de redes sociales que criticaban al gobierno indonesio**, lo que causó preocupación a los internautas y activistas. Por ejemplo, un usuario recibió una advertencia tras publicar un vídeo en el que criticaba la aplicación irregular de los protocolos de distanciamiento social de Covid-19. En dicho video, superponía imágenes de las multitudes que se congregaron en Nusa Tenggara Oriental durante una visita presidencial con vídeos de vendedores ambulantes obligados a cerrar sus puestos.

El uso de las leyes sobre ciberdelincuencia para perseguir a quienes difunden información controvertida sobre el Covid-19 debe considerarse dentro de un contexto más amplio en el que **estas mismas leyes se están utilizando para limitar indebidamente la libertad de expresión y reprimir las voces disidentes**, incluidas las de periodistas y activistas, pero también las de las personas que intentan expresar su opinión política. Por ejemplo, en Arabia Saudí, Salma al-Shehab fue condenada recientemente a 34 años de prisión por difundir mensajes de activistas y exiliados que pedían la liberación de presos políticos. Según una investigación de *The Guardian*, "no era una activista saudí destacada ni particularmente vocal", y sólo tenía 2.597 seguidores en Twitter. Este caso ejemplifica cómo **se puede abusar de las leyes sobre**

CASO DE KENIA

Criminalización de la disidencia bajo el pretexto de luchar contra la desinformación sobre el Covid-19

Informe de la Kenya Human Rights Commission – KHRC

El Estado utilizó la ley sobre uso indebido de la informática y los delitos cibernéticos de 2018 para **castigar a blogueros y voces disidentes por la supuesta publicación de información engañosa** sobre el estado de preparación y la respuesta del gobierno frente al Covid-19. Cualquier persona que publicara información sobre el Covid-19 en internet se arriesgaba a infringir la ley, cuyos artículos 23 y 24 establecen sanciones penales de dos y diez años, respectivamente.

Expertos en derechos humanos condenaron la detención ilegal y el procesamiento, en virtud de esta ley, del defensor de los derechos humanos Edwin Mutemi wa Kiama, que criticó en internet al gobierno keniano por el préstamo que solicitó al Fondo Monetario Internacional (FMI) para hacerle frente al Covid-19, en medio de la frustración por la carga de la deuda y la corrupción de Kenia. La detención de Kiama forma parte de una tendencia preocupante que surge de la incorrecta aplicación de la ley sobre uso indebido de la informática y los delitos cibernéticos de 2018 con el objetivo de controlar desproporcionadamente la libertad de expresión. Tras numerosas intervenciones de actores de la sociedad civil, Kiama fue liberado definitivamente el 20 de abril de 2021 por falta de pruebas que demostraran que había infringido determinadas disposiciones de esta ley con características represivas. A lo largo de la pandemia, el gobierno siguió utilizando esta ley como herramienta para reprimir la libertad de expresión.

ciberdelincuencia para censurar políticamente las redes sociales que se han convertido en importantes lugares de activismo y compromiso cívico. La pandemia de Covid-19 ha creado otra justificación para que los gobiernos represivos extiendan estos poderes y amplíen los tipos de discurso que consideran perjudiciales para la seguridad nacional.

Más facultades para los servicios de inteligencia

Otra tendencia en la vigilancia en torno a la pandemia fue la **autorización especial que recibieron los servicios de inteligencia nacionales para llevar a cabo actividades de vigilancia nacional.** Por ejemplo, el gobierno israelí, para hacer frente a la pandemia, recurrió a su agencia de servicios secretos, Shin Bet. En marzo de 2020, el Primer Ministro Benjamin Netanyahu anunció que había autorizado a los servicios de inteligencia Shin Bet para rastrear los movimientos de los pacientes infectados con el fin de descubrir con quién habían estado en contacto. Esta búsqueda retroactiva requería que los agentes de seguridad accedieran a lo que el *New York Times* denominó "un gran tesoro de datos de teléfonos móviles que no había sido revelado hasta la fecha", los cuales se habían recopilado de forma encubierta con el objetivo de luchar contra el terrorismo. En otras palabras, la respuesta del gobierno de Netanyahu a la pandemia reveló información nueva sobre el alcance de la vigilancia masiva de los servicios de inteligencia israelíes, que se extiende a todos y cada uno de los usuarios de teléfonos móviles del país. El Tribunal Superior de Israel no tardó en condenar esta práctica.

En Pakistán, el gobierno adaptó un sistema que una agencia de espionaje militar - los Servicios de Inteligencia Conjunta (ISI, por sus siglas en inglés)- había desarrollado, originalmente, con fines antiterroristas, para vigilar la propagación del Covid-19. Aunque se desconoce el mecanismo exacto que impulsó este sistema, aparentemente, una herramienta que originalmente había sido diseñada para rastrear terroristas a partir de datos de geolocalización celular, fue adaptada para rastrear casos de Covid-19. El uso de herramientas de seguridad nacional con fines civiles y la mayor dependencia de los ISI generan preocupación debido a que los defensores de los derechos humanos han acusado a la agencia de espionaje militar de "graves violaciones de los derechos humanos", entre ellas la tortura y el asesinato de periodistas, críticos anti militares y activistas políticos. Según Hija Kamran, defensora paquistaní de los derechos digitales, "la intervención de los ISI en el rastreo y la localización, la falta de información sobre la tecnología o el método que utilizan para vigilar y rastrear a los sospechosos, y la presión para que los usuarios registren sus VPN son todos **puntos interconectados que apuntan hacia un gran objetivo: la disminución de la privacidad y la capacidad de rastrear a todos los ciudadanos.**"

Debemos considerar el uso de los servicios de inteligencia nacionales y las agencias de espionaje militar en relación con una tendencia más amplia en las respuestas globales a la pandemia: la securitización de la salud nacional. En todo el mundo, las fuerzas militares y de seguridad recibieron poderes extraordinarios para imponer toques de queda y confinamientos, lo que dio lugar a un uso excesivo de la fuerza en al menos 18 países, donde las fuerzas militares y policiales "agredieron físicamente a periodistas, blogueros y manifestantes, incluidas algunas personas que criticaban las respuestas gubernamentales al Covid-19", según un informe de Human Rights Watch de 2021. Los informes de nuestros investigadores asociados reportaron casos de uso excesivo y letal de la fuerza por parte de las fuerzas militares para hacer cumplir la cuarentena, que resultaron en hospitalizaciones en Indonesia y muertes en Sudáfrica y Kenia. Estos incidentes demuestran la necesidad de rendición de cuentas por parte de los gobiernos y de proporcionalidad en la aplicación de la ley cuando hay una crisis de salud pública. Aunque estos casos de violencia no parecen estar directamente relacionados con ninguna tecnología o medida de vigilancia en particular, revelan las **graves consecuencias que puede tener el despliegue de poderes extraordinarios sin garantías**. También demuestran la predisposición de los Estados a utilizar la fuerza durante una emergencia sanitaria nacional, lo cual constituye un precedente preocupante que podría **intensificarse si se combina con tecnologías de vigilancia poderosas.**

La profesora Fionnuala Ní Aoláinm, Relatora Especial de las Naciones Unidas sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, ha resaltado la insensatez de confiar en el sector encargado de la seguridad para gestionar necesidades complejas de salud pública. Los sistemas antiterroristas son conocidos por eludir los derechos humanos, atacar ilegalmente a grupos de la sociedad

civil (minorías étnicas, religiosas y de otros tipos), por su falta de transparencia y rendición de cuentas y sus prácticas encubiertas. Estas mismas preocupaciones aparecen cuando las leyes y tecnologías antiterroristas se adaptan para cumplir nuevos objetivos. En los ejemplos anteriores, hemos visto cómo los gobiernos han ampliado la interpretación de la "seguridad nacional" para incluir la respuesta a la pandemia y han utilizado las leyes y tecnologías antiterroristas para vulnerar la privacidad de las personas, así como las libertades de expresión, circulación y reunión.

En resumen, nuestras principales preocupaciones relacionadas con la adaptación de las medidas de seguridad existentes para fines de vigilancia son las siguientes:

1. El incremento de la vigilancia y la censura de la sociedad civil mediante la adaptación de la legislación antiterrorista.
2. El despliegue de tecnologías militares o antiterroristas contra la población, lo cual vulnera derechos fundamentales, incluido el derecho a la privacidad.
3. El uso excesivo de la fuerza sobre la población mientras se llevan a cabo medidas de vigilancia de emergencia.

Tendencia nro. 2: El silenciamiento de la sociedad civil

La libertad de expresión y de opinión son temas que adquirieron una especial relevancia durante la pandemia, ya que los gobiernos trataron de limitar la difusión de información errónea y la desinformación relacionadas con el Covid-19. Aunque la información falsa es suficiente para generar una preocupación legítima sobre la seguridad pública, **algunos gobiernos utilizaron el pretexto de combatir la desinformación como justificación para censurar la expresión y eliminar la crítica.**

El efecto disuasorio de las sanciones penales

En la Tendencia nro. 1, analizamos cómo algunos gobiernos invocaban las leyes de ciberdelincuencia para restringir la libertad de expresión. Otros países intentaron obtener resultados similares mediante estrategias legales diferentes. Por ejemplo, Rusia implementó cambios en su Código Penal "introduciendo sanciones penales por la 'difusión pública de información falsa a sabiendas' en el contexto de emergencias, y sanciones administrativas para los medios de comunicación que publicaran dicha información". Por otro lado, Filipinas aprobó una ley por la que se declaraba el estado de emergencia, la cual incluía una disposición que penalizaba la difusión de "información falsa". El gobierno sudafricano legisló y criminalizó la desinformación a través del Reglamento de la Ley de Gestión de Desastres de 2002, el cual otorgaba al gobierno el fundamento jurídico necesario para penalizar a quienes publicaran declaraciones a través de cualquier medio, incluidas las redes sociales, con la intención de engañar a otros sobre el Covid-19, el estado de infección por Covid-19 de cualquier persona, o cualquier medida adoptada por el gobierno para hacer frente al Covid-19. Los infractores se enfrentaban a penas desproporcionadas, incluida la pena de prisión de hasta seis meses. Estas penas extremas y desproporcionadas pueden afectar a la sociedad civil, especialmente cuando se utilizan como pretexto para reprimir las críticas sobre las políticas del gobierno. Esta táctica se utilizó contra activistas en Camboya, Irán, India y Tailandia, según observadores de derechos humanos e informes de los medios de comunicación.

En Argentina, las "patrullas cibernéticas" vigilaron la actividad en las redes sociales para determinar el "estado de ánimo" con respecto a la pandemia, lo que consideraron fundamental para prevenir disturbios. Cualquier persona declarada culpable de "intimidación pública" podía ser condenada a hasta seis años de prisión. Al finalizar el primer mes del confinamiento obligatorio, al menos 12 personas habían sido acusadas de "intimidación pública" como consecuencia de la difusión de información errónea que, según el Jefe de la Unidad Fiscal Especializada en Ciberdelincuencia, podía "llevar a incitar a la violencia colectiva".

En Argentina y en otros países hubo poca transparencia sobre los criterios utilizados para definir el alcance de los términos "desinformación" o "noticias falsas", o sobre si tales criterios existían siquiera. Esta **falta de transparencia conduce a una aplicación arbitraria de la ley y dificulta la defensa de las personas acusadas de difundir información falsa**. La vaguedad y ambigüedad en torno a términos como "intimidación pública" puede llevar a situaciones como la de Kevin Guerra, un joven argentino de 20 años que se convirtió en objeto de una investigación penal tras publicar un comentario sarcástico en Twitter cuando aún no había cobrado el Ingreso Familiar de Emergencia que le correspondía. Las **sanciones penales de este tipo pueden tener un efecto disuasorio sobre la expresión**, limitando la voluntad de las personas de expresarse, incluso de forma satírica.

Espacios públicos bajo vigilancia

Otra de las principales tendencias que observamos fue **el uso de tecnología de vigilancia para controlar los espacios públicos** con la justificación de hacer cumplir la cuarentena y el distanciamiento social. Por ejemplo, en Túnez, un robot teledirigido patrullaba las calles, exigiendo a los transeúntes que mostraran sus documentos de identidad a una cámara, mientras que la policía desplegó drones en Australia, Francia, Grecia e India. Además, en Kenia y Moldavia, los gobiernos utilizaron imágenes obtenidas por cámaras de videovigilancia y tecnología de reconocimiento facial para vigilar los espacios públicos y hacer cumplir los requisitos de distanciamiento social. El uso de tecnologías de vigilancia en espacios públicos era, y sigue siendo, profundamente intrusivo, especialmente cuando se lo combina con sistemas de reconocimiento facial. Generalmente, las personas que

circulan por espacios públicos no son conscientes de que se captura su imagen o no tienen la posibilidad de consentirlo; además, rara vez pueden acceder a información sobre cómo se almacenan sus imágenes o quién las utiliza.

El uso de tecnologías de vigilancia para patrullar el espacio público debe considerarse dentro de un contexto más amplio en el que las protestas pacíficas estaban siendo estrechamente vigiladas, lo que en algunos casos llevaba a que fueran dispersadas por la fuerza -en algunos casos violentamente- bajo el pretexto de que estaban infringiendo las normas de distanciamiento social. Por ejemplo, en Kenia hubo manifestantes que fueron detenidos por no respetar las normas de Covid-19 que prohibían las concentraciones públicas. Sin embargo, los observadores locales de derechos humanos consideraron que estas detenciones respondían a cuestiones políticas, ya que las normas de distanciamiento social se aplicaban de forma desigual y los políticos podían celebrar actos de campaña que congregaban a multitudes, a pesar de que las elecciones generales no estaban previstas hasta 18 meses después. En Polonia, los líderes de las protestas masivas de octubre de 2020 contra la prohibición casi absoluta del aborto están siendo procesados por "constituir una amenaza epidemiológica". El uso de tecnologías de vigilancia en el espacio público, especialmente cuando las aplican gobiernos con un historial de represión de la disidencia, puede tener un **efecto disuasorio sobre las libertades de expresión, reunión y asociación**.

En resumen, nuestras principales preocupaciones relacionadas con el silenciamiento de la sociedad civil son las siguientes:

1. El uso de tecnologías de vigilancia intrusivas en espacios públicos, que tienen un efecto disuasorio sobre las libertades de expresión, reunión y circulación.
2. Las sanciones penales, introducidas bajo el pretexto de acabar con la desinformación, utilizadas contra la sociedad civil.

CASO DE FRANCIA

Vigilancia ilegal con drones

Informe de La Quadrature du Net

A partir del primer confinamiento, la policía empezó a utilizar drones para vigilar a la población. Estos drones de vigilancia pertenecían a la policía desde hacía muchos años, pero su uso era mínimo y no había recibido mucha cobertura mediática. Estos drones circulaban por las calles de ciudades francesas medianas y grandes, dependiendo del equipamiento de la policía local. Generalmente, estaban equipados con parlantes que les indicaban a las personas, que estaban siendo filmadas, que regresaran a sus casas (a pesar de que no estaba prohibido salir, ya que existían muchas excepciones).

En mayo de 2020, La Quadrature du Net (LQDN) cuestionó el uso de drones en París, donde la prensa había podido recabar cierta información técnica que podía servir para demostrar la existencia de un tratamiento ilegal de datos ante la justicia. LQDN ganó el caso ante el Conseil d'État, el cual dictaminó que los drones estaban procesando datos personales sin ningún fundamento jurídico.

Aunque la mayoría de las fuerzas policiales locales dejaron de utilizar drones de vigilancia en mayo de 2020, tras la victoria de LQDN, la policía de París continuó intentando utilizar estas tecnologías. Aun cuando el confinamiento casi había finalizado, se documentó la vigilancia de manifestaciones entre mayo de 2020 y octubre de 2020. En octubre de 2020, LQDN volvió a cuestionar a la policía de París por utilizar drones de vigilancia para vigilar protestas. El uso de drones volvió a ser declarado ilegal en diciembre de 2020.

Tendencia nro. 3: El riesgo del uso indebido de datos personales

Como respuesta al Covid-19, y a los fines de controlar la propagación del virus, gobiernos de todas partes del mundo implementaron diversas tecnologías de vigilancia como las aplicaciones de rastreo de contactos, certificados digitales de vacunas, pulseras electrónicas, seguimiento de tarjetas SIM o la identificación biométrica. En muchos países, sin embargo, la falta de transparencia y rendición de cuentas de los organismos estatales sobre la recopilación y el uso de datos personales genera serias dudas sobre la **legitimidad de la injerencia en el derecho a la privacidad y sobre el impacto que la recopilación excesiva de datos podría tener en los actores de la sociedad civil**. Muchos países no tenían leyes de protección de datos y, los que sí, utilizaron exenciones y excepciones para eludirlas. La falta de claridad sobre el fundamento jurídico y los fines de la recopilación de datos, así como la inexistencia de garantías y mecanismos de supervisión para evitar el uso indebido de los datos, generan una legítima preocupación sobre si las herramientas de vigilancia digital adoptadas en nombre de la lucha contra la propagación del virus pueden ser utilizadas para atacar a los activistas o limitar el ejercicio de los derechos civiles.

Intromisiones ilegales en la privacidad: Falta de claridad con respecto a los fines de las aplicaciones relacionadas con el Covid-19 y las garantías aplicables

Muchos gobiernos implementaron aplicaciones móviles de rastreo de contactos que recopilaban datos de localización de los usuarios a través de la señal celular o de Bluetooth. En 2021, un grupo de analistas de seguridad descubrió que las aplicaciones de rastreo de contactos estaban operativas en más de 90 países. Las aplicaciones móviles también se utilizaban para rastrear síntomas y mostrar pruebas de vacunación o recuperación para poder acceder a espacios cerrados o viajar. Estas aplicaciones se pusieron en funcionamiento sin una evaluación previa del marco jurídico que las regula, de su eficacia o de la existencia de garantías adecuadas. Los datos recogidos por estas aplicaciones eran muy diversos. Algunas aplicaciones combinaban el rastreo de ubicación con un registro biométrico, como en Australia o Polonia, donde las personas a las que se les había

CASO DE INDONESIA

Las malas prácticas de almacenamiento de datos dejan desprotegidos a los datos personales de los usuarios

Informe de KontraS

Para hacer frente al brote de Covid-19, el Ministerio de Salud indonesio creó la aplicación PeduliLindung, que se lanzó a principios de julio de 2021. La aplicación PeduliLindung se utilizó para controlar la ubicación de las personas, así como para proporcionar información a la población indonesia sobre las zonas rojas de Covid-19 en diversas partes de Indonesia, las vacunas y certificados obligatorios, los resultados de las pruebas de Covid-19 y las certificaciones necesarias para poder acceder a los servicios públicos.

Otra función de esta aplicación era la llamada Tarjeta Electrónica de Alerta Sanitaria (eHAC, por sus siglas en inglés). La función específica de la eHAC era que el Ministerio de Salud indonesio recopilara datos sobre las personas que querían viajar, tanto dentro como fuera del país. Cabe señalar que la eHAC se volvió obligatoria para cualquier persona que pretendiera viajar, especialmente para quienes cruzaban fronteras regionales o estatales, así como para los extranjeros que ingresaban al país.

Al ingresar en la aplicación, se les solicitaba a los usuarios sus datos personales (como nombre, número de residencia (NIK), dirección, fotografía, número de teléfono, dirección de correo electrónico, entre otros), sin que existiera ninguna garantía de la protección de datos.

Lamentablemente, los datos recopilados no se mantuvieron seguros. En agosto de 2021, los investigadores Noam Rotem y Ran Locar revelaron una falla de seguridad que dejaba al descubierto toda la infraestructura en torno al eHAC y "dejaba expuestos en un servidor abierto los datos de más de un millón de personas", incluidos los datos personales de funcionarios indonesios y registros de hospitales privados. Los investigadores también encontraron datos personales, desde números de identidad nacionales, números de teléfono, resultados de pruebas Covid-19 e información relativa a la ubicación.

La filtración de datos del eHAC confirma que el gobierno no garantizó la seguridad de todos los usuarios en el ejercicio de sus derechos digitales. No era la primera vez que se filtraban datos gubernamentales. Previamente, el gobierno tampoco había garantizado la seguridad de la información del seguro nacional de salud y la información electorales. Las principales causas son la mala gestión de los sistemas y la inadecuada infraestructura de seguridad, así como la falta de una ley de protección de datos.

diagnosticado Covid-19 debían participar en registros aleatorios de reconocimiento facial para garantizar que cumplían las normas de la cuarentena. En general, **las aplicaciones de Covid-19 se desarrollaron e implementaron rápidamente.** Muchos usuarios informaron fallos en el software y falsas alarmas. Además, los estudios de casos realizados por las organizaciones locales de la sociedad civil que participaron en este informe confirmaron que sus gobiernos no comunicaron adecuadamente cómo funcionaban las aplicaciones de rastreo de contactos, qué información recopilaban o cómo se analizaba, utilizaba, almacenaba y compartía esta información.

Preocupaciones relativas al Estado de Derecho

Una cuestión relacionada con este asunto es que la **recopilación de datos resultó desproporcionada en relación con el objetivo de frenar la propagación del Covid-19 y, en algunos casos, careció de fundamento jurídico** (como se detalla más adelante en este informe). Por ejemplo, en la India, el marco legal que regulaba el uso de la aplicación de rastreo de contactos estaba compuesto en su totalidad por **legislación delegada, en lugar de primaria**, mientras que en Francia la justicia sostuvo que el gobierno estaba procesando datos obtenidos a través de drones de vigilancia **sin un fundamento jurídico legítimo** (como se desarrolló anteriormente en este informe). Si a esto se suma la falta general de transparencia y rendición de cuentas relativas a la recopilación de datos, algunos usuarios temen que sus datos puedan ser reutilizados para objetivos distintos a los originales o almacenados indefinidamente de forma que puedan causar daños en el futuro.

Predicciones erróneas y pocas vías de reparación

En algunos casos, los datos recopilados por las aplicaciones móviles se **utilizaron para hacer predicciones sobre la salud de las personas mediante procesamiento automatizado, incluyendo machine learning (aprendizaje automático)**. Además, algunos Estados utilizaron sistemas algorítmicos de toma de decisiones para determinar quién debía recibir vacunas o qué personas podían solicitar las prestaciones de asistencia para situaciones de emergencia. Por ejemplo, PanaBIOS, una aplicación utilizada en el control fronterizo de Ghana y respaldada por la Unión Africana, sostuvo que utilizaba

CASO DE COLOMBIA

Falta de transparencia de la aplicación de rastreo de contactos

Informe de Dejusticia

En marzo de 2020, pocos días después de que la Organización Mundial de la Salud declarara la pandemia de Covid-19, el gobierno colombiano lanzó una aplicación móvil llamada CoronApp, siguiendo el ejemplo de Corea del Sur y Singapur (primeros países en implementar tecnologías de vigilancia para controlar la propagación del virus). En el caso colombiano, sin embargo, no se trataba de una tecnología nueva. De hecho, el gobierno renombró una aplicación de código abierto que existía desde 2017. La aplicación fue diseñada, originalmente, para monitorear la salud pública en Colombia durante la visita del Papa Francisco.

Al principio, el objetivo principal de CoronApp era permitirle a la población estar informada sobre la evolución de la pandemia en Colombia. Sin embargo, con posterioridad, la narrativa en torno a la aplicación cambió. Su propósito se hizo más ambicioso. Pronto se convirtió en una herramienta digital para mantener informada a la población y "salvar tantas vidas como fuera posible".

Esta nueva narrativa permitió la rápida introducción de nuevas funcionalidades en la aplicación que, en teoría, permitirían al gobierno alcanzar sus ambiciosos objetivos. La función original -proporcionar información fiable sobre la pandemia- se complementó con otras: un sistema digital de rastreo de contactos, un cuestionario para declarar los síntomas relacionados con el Covid-19 y un pasaporte digital de movilidad.

El rastreo de contactos se implementó sin transparencia sobre a qué datos tenía acceso la aplicación o qué funcionalidades del celular eran necesarias para su funcionamiento. Sin embargo, los análisis técnicos realizados por organizaciones locales de la sociedad civil determinaron que CoronApp tenía acceso a los datos GPS, Bluetooth y Wi-Fi de los dispositivos en los que estaba instalada. Aunque el gobierno tuvo acceso a los datos de CoronApp desde marzo de 2020, los usuarios no fueron informados de esa situación hasta abril. El gobierno tampoco informó qué entidades públicas tenían acceso a la información recopilada por CoronApp ni cómo la recopilación de esta información era útil para controlar la propagación del virus. No hubo transparencia sobre cómo se almacenaban los datos ni durante cuánto tiempo.

El almacenamiento de cantidades masivas de datos sin un objetivo claro tiene, de por sí, un impacto negativo sobre la privacidad y otros derechos civiles. Sin embargo, en opinión de Dejusticia, es muy probable que el gobierno utilizara los datos personales recopilados durante la pandemia para servir a los intereses comerciales de las empresas públicas, ya que necesitaban continuar funcionando. De acuerdo con documentos públicos revelados durante el curso de litigios estratégicos impulsados por organizaciones de la sociedad civil, una cantidad inesperada de terceros tuvieron acceso a la base de datos de CoronApp: empresas de la industria del gas y el petróleo, el Departamento Administrativo de la Presidencia y la Empresa de Teléfonos de Bogotá. Los usuarios no tenían conocimiento de esta práctica.

"algoritmos para rastrear y localizar a las personas que se enfrentan a posibles amenazas para la salud y llevar un registro de las muestras analizadas desde su origen hasta llegar a los laboratorios nacionales". Los usuarios no tenían claro cómo se recopilaban y compartían los datos. Más allá de las preocupaciones tradicionales en materia de transparencia y rendición de cuentas asociadas a las aplicaciones de rastreo de contactos, hay un elemento adicional de incertidumbre cuando los datos de los usuarios son procesados por herramientas de análisis predictivo o de evaluación de riesgos. Esto se debe a que **los usuarios rara vez reciben información sobre cómo se toman las decisiones automatizadas y cuentan con pocas vías de reparación**. En julio de 2022, hubo viajeros que denunciaron que la aplicación ArriveCAN, requerida para cruzar la frontera canadiense, les indicaba, incorrectamente, que debían realizar cuarentena. Un portavoz de la Agencia de Servicios de Fronteras de Canadá confirmó que habían "identificado un fallo técnico en la aplicación" que "puede generar una notificación errónea indicando a la gente que realice cuarentena." El caso de la aplicación ArriveCAN demuestra la falta de rendición de cuentas en torno a estas aplicaciones y los efectos perjudiciales que pueden tener las predicciones falsas en la vida de las personas. Cuando las aplicaciones producen falsos positivos, esto puede dar lugar a confusión y desconfianza en las autoridades públicas. Esto sucedió en septiembre de 2020, cuando un establecimiento educativo irlandés tuvo que cerrar sus puertas a más de la mitad de sus alumnos luego de que más de 30 de sus profesores recibieran una falsa alerta de contacto estrecho a través de la app irlandesa de rastreo de contactos.

En resumen, nuestras principales preocupaciones relacionadas con el riesgo del uso indebido de datos personales son:

1. La enorme recopilación de datos personales, incluidos datos sensibles, sin justificación ni fundamento jurídico, que es desproporcionada en relación con el objetivo establecido originalmente, lo cual resulta en una grave amenaza de uso indebido de datos, incluido el riesgo de que los activistas se conviertan en objetivos.
2. La falta de transparencia y rendición de cuentas en la recopilación, el uso e intercambio de datos personales, que genera preocupación por la adaptación de la tecnología y el uso de los datos con fines comerciales.
3. La falta de transparencia en torno a los sistemas predictivos basados en el aprendizaje automático y el procesamiento automatizado, sin acceso a vías de reparación.

Tendencia nro. 4: El influyente papel de las empresas privadas

Las empresas privadas desempeñaron un papel importante en muchas de las respuestas de los países frente al Covid-19, a través de acuerdos de intercambio de datos o del desarrollo de aplicaciones de localización de contactos y pasaportes digitales. En los primeros días de la pandemia, los gobiernos les pidieron a empresas privadas, como operadores de telecomunicaciones y servicios de taxi, que compartieran los datos de localización de los usuarios. Algunas leyes que obligaban a las empresas a compartir datos de telecomunicaciones con organismos estatales fueron anuladas por tribunales constitucionales o autoridades de protección de datos, como es el caso de Eslovaquia, Bulgaria, Alemania y Eslovenia. El intercambio de datos entre entidades públicas y privadas fue en ambos sentidos; por ejemplo, en el Reino Unido, el gobierno compartió datos sensibles de pacientes con empresas para que los procesaran y analizaran.

Colaboraciones poco claras entre los sectores público y privado

El procesamiento de datos y otras relaciones entre gobiernos y empresas privadas fueron, en muchas ocasiones, turbios. En algunos países, el público recibió poca información o información contradictoria sobre el alcance de estas asociaciones, lo que generó dudas sobre cuáles eran las partes responsables de conservar los datos y durante cuánto tiempo, qué ocurrirá con los datos una vez finalizada la asociación y si los usuarios podían estar seguros de que sus datos no se utilizarían indebidamente para actividades de marketing o con fines de lucro. Otra preocupación es que los datos sensibles puedan utilizarse para entrenar algoritmos de aprendizaje automático y producir software que será propiedad de la empresa. Sin suficiente transparencia sobre los acuerdos celebrados entre gobiernos y empresas privadas, es difícil saber quién debe responder en caso de violación de datos. Asimismo, cuando los gobiernos externalizan las tareas de procesamiento y almacenamiento de datos, "los ciudadanos pierden gran parte de su poder para hacer rendir cuentas a los gobiernos: el gobierno renuncia y transfiere la responsabilidad a actores privados frente a los que los ciudadanos tienen menos derechos".

La influencia del sector privado en el establecimiento de estándares universales en situaciones de crisis

Una de las intervenciones más impactantes del sector privado fue la interfaz de programación de aplicaciones (API, por sus siglas en inglés) conocida como Sistema de Notificación de Exposición Google/Apple (GAEN), una estructura de trabajo sobre el que pueden desarrollarse aplicaciones de rastreo de contactos. La API GAEN, que funciona a través de Bluetooth y que se utilizó en casi 40 países, sirvió como base para ayudar a los gobiernos locales, regionales y nacionales a crear sus propias aplicaciones de rastreo de contactos. La API fue muy popular, ya que los gobiernos se vieron presionados para desarrollar rápidamente aplicaciones móviles para la localización de contactos, y esta API garantizaba la compatibilidad con los dispositivos móviles que utilizan los sistemas operativos de Google y Apple (Android e iOS, respectivamente). Como explicó Marcel Salathé, epidemiólogo digital que trabajó en el desarrollo de la aplicación SwissCovid: "Quieren tener una herramienta que funcione en los teléfonos de los usuarios, y Google y Apple controlan el 99,5% de los sistemas operativos". Los países que intentaron crear sus propias aplicaciones se enfrentaron con obstáculos por el hecho de que los sistemas operativos de Google y Apple restringen la difusión Bluetooth en segundo plano, lo que **reduciría la eficacia de cualquier aplicación desarrollada sin la cooperación de los gigantes tecnológicos**. Esta es, probablemente, la razón por la que tanto Alemania como el Reino Unido abandonaron las aplicaciones desarrolladas de forma independiente para pasarse al sistema GAEN API. La popularidad de la API GAEN plantea **serias dudas sobre el poder de las empresas privadas para determinar las respuestas a la pandemia y establecer estándares universales en medio de una crisis de salud pública**. La enorme influencia de Google y Apple, y su capacidad para imponer estándares de rastreo de contactos a gobiernos de todo el mundo, genera serias dudas sobre la supervisión democrática y la rendición de cuentas.

Asimismo, los investigadores han puesto en duda que la API GAEN proteja la privacidad de los usuarios de manera adecuada. Un estudio demostró que, en el caso de los usuarios de teléfonos Android, la aplicación irlandesa de rastreo de contactos GAEN requería la activación de Google Play Services y, por tanto, enviaba datos a los servidores de Google cada 20 minutos. El mismo grupo de

CASO DE SUDÁFRICA

Preocupación por la privacidad debido a la excesiva dependencia de WhatsApp

Informe del Legal Resources Centre

Las principales tecnologías que el gobierno sudafricano implementó para controlar la propagación del Covid-19 fueron la aplicación COVID Connect, que se lanzó en julio de 2020, y la aplicación COVID Alert SA, que se lanzó en septiembre de 2020 como la aplicación oficial de Sudáfrica para notificar la exposición al virus y permitir el rastreo de contactos. COVID Connect comenzó como un canal de WhatsApp para proporcionar información fiel sobre el Covid-19. En los meses siguientes, COVID Connect se convirtió en un servicio que proporcionaba información sanitaria, así como herramientas de detección y rastreo de contactos. COVID Alert SA se lanzó como una aplicación que funcionaría junto con COVID Connect. La aplicación COVID Alert SA se basa en la API Sistema de Notificación de Exposición Google/Apple (Google/Apple Exposure Notification – GAEN, por sus siglas en inglés) y funciona a través de Bluetooth, enviando notificaciones de exposición a los usuarios si han estado en contacto estrecho con otro usuario de la aplicación que ha dado positivo en la prueba de Covid-19.

Los revisores técnicos nombrados por el grupo de interés público ALT Advisory examinaron las dos aplicaciones implementadas por el Covid-19 en Sudáfrica y expresaron su preocupación por la dependencia de WhatsApp como plataforma de comunicación. Los revisores técnicos explicaron que el uso de la interfaz de programación de aplicaciones (API) de WhatsApp para notificar los resultados de sus pruebas de Covid-19 a los usuarios de la aplicación COVID Alert SA, genera preocupaciones con respecto a la privacidad, independientemente de lo conveniente que pueda resultar. Este enfoque les permite, potencialmente, a terceros con intereses comerciales identificar qué usuarios han sido diagnosticados como Covid-19 positivos. Ésta no es una exigencia del sistema GAEN, por lo que parece haber sido una elección de los desarrolladores. Aunque el contenido de los mensajes está cifrado, cabe prever que se puedan extraer suposiciones -como en qué fase de recuperación del Covid-19 se encuentra una persona- cuando un usuario de la aplicación se pone en contacto con el Departamento Nacional de Salud a través de WhatsApp.

investigadores descubrió que Google recibía periódicamente "números de serie de tarjetas SIM y hardware, IMEI del teléfono, dirección MAC y dirección de correo electrónico del usuario de Google, junto con información detallada sobre otras aplicaciones que se ejecutaban en el teléfono". Otras cuestiones incluyen la posibilidad de ciberataques y falsas alertas positivas que proporcionan información incorrecta sobre la exposición al Covid-19. Si se tiene en cuenta la cuestionable precisión de las aplicaciones de rastreo de contactos basadas en la API GAEN, la fuga de datos resulta más preocupante, ya que los usuarios pueden haber puesto en peligro sus datos personales al utilizar una aplicación que ni siquiera cumple el objetivo original de reducir la exposición al Covid-19.

Asimismo, hay una cuestión de transparencia. En este sentido, los autores del estudio Android/GAEN resaltaron la gran discrepancia entre el considerable escrutinio público que recibió la aplicación por pertenecer a las autoridades sanitarias irlandesas (incluida una evaluación de impacto sobre la protección de datos), y la falta de documentación pública sobre el componente GAEN de la misma aplicación. Llegaron a la conclusión de que "dado que muchos gobiernos están animando a poblaciones enteras a utilizar estas aplicaciones, es necesario que los detalles de su funcionamiento sean accesibles para que los usuarios de estas aplicaciones, tanto actuales como potenciales, puedan tomar decisiones informadas".

En resumen, nuestras principales preocupaciones en relación con el papel de las empresas privadas son las siguientes:

1. El acceso ilegal de los organismos estatales a los datos provenientes de telecomunicaciones y otros datos proporcionados a empresas privadas.
2. La falta de transparencia sobre los acuerdos de tratamiento de datos entre los sectores público y privado, así como sobre las garantías aplicables, que conducen a posibles usos indebidos de datos.
3. La falta de escrutinio público de las herramientas del sector privado como parte de las respuestas estatales, lo que lleva a que las empresas privadas utilicen los datos para sus propios intereses.
4. La reivindicación de las responsabilidades del Estado, que les permiten a las empresas privadas establecer estándares universales en medio de una crisis de salud pública, lo que plantea riesgos potenciales para la supervisión democrática y la rendición de cuentas.

Tendencia nro. 5: La normalización de la vigilancia más allá de la pandemia

La mayoría de las medidas de vigilancia relativas al Covid-19 se introdujeron durante el primer año de la pandemia. En el momento de redactar este informe, en la segunda quincena de noviembre de 2022, podemos observar cómo algunas de estas medidas extraordinarias se han ampliado o cómo los datos recopilados bajo el pretexto de luchar contra el Covid-19 se han utilizado para otros fines. Nuestra mayor preocupación es que **la pandemia ha abierto las puertas para que la vigilancia gubernamental invasiva sea normalizada, incluso luego de que la amenaza del virus haya disminuido**.

Debemos considerar la readaptación de la infraestructura desarrollada alrededor del Covid-19 en relación con **la tendencia más amplia hacia la vigilancia gubernamental excesiva tras emergencias nacionales**, bajo la lógica de que la seguridad sólo puede lograrse acumulando cada vez más información. El ejemplo más destacado de esta tendencia es la ampliación de los poderes de vigilancia de los gobiernos tras los atentados terroristas del 11 de septiembre en EE.UU., que estableció una infraestructura mundial de recopilación invasiva de datos que sigue estando vigente 20 años después, a pesar de los informes sobre los escasos o nulos beneficios que tuvieron en la lucha contra el terrorismo.

La readaptación de las aplicaciones de Covid-19 para nuevos fines

En Guatemala, por ejemplo, el gobierno lanzó una aplicación llamada *Alerta Guate* para difundir información sobre salud pública. Aunque la finalidad original de la aplicación era brindar información sobre el Covid-19, en marzo de 2020, el Presidente Alejandro Giammattei declaró que "también tendrá otras funciones" y que la población debería seguir utilizando la aplicación después de que la pandemia remitiera para recibir información sobre "cuestiones de seguridad" y para ayudar en la búsqueda de niños desaparecidos. Los comentarios de Giammattei revelan que, ya los primeros días tras el lanzamiento de la aplicación, la Presidencia consideraba usos alternativos para la tecnología. La ampliación de los fines de la aplicación Alerta Guate es un **excelente ejemplo de "mission creep"**, un término que describe la adaptación de una medida o herramienta para servir a objetivos distintos de aquellos para los que fue originalmente diseñada. Además, los activistas de la privacidad expresaron su preocupación por el hecho de que la aplicación Alerta Guate "pide permiso para acceder a archivos, llamadas y audio" y recopila información del usuario, incluidos datos de localización, cuentas de redes sociales e "intereses personales", que se conserva durante diez años. La excesiva recopilación y almacenamiento de datos, combinada con una tendencia a la modificación de los objetivos originales, son especialmente preocupantes en el contexto guatemalteco, un país en el que el gobierno ha llevado a cabo, históricamente, una vigilancia de alta tecnología contra "políticos, periodistas, diplomáticos y líderes sociales" y en el que los ataques contra los defensores de los derechos humanos alcanzaron niveles históricos en 2020. Por esta razón, el Procurador de los Derechos Humanos de Guatemala, Jordán Rodas Andrade, arremetió contra la aplicación Alerta Guate, calificándola de "sumamente riesgosa para la salud de la democracia y las libertades civiles".

Los gobiernos de Colombia, India y Kenia han anunciado planes similares para **seguir utilizando las aplicaciones implementadas durante la pandemia para fines no relacionados con la emergencia**. Tras la suspensión de la emergencia sanitaria nacional en julio de 2022, el gobierno colombiano cambió el nombre de CoronApp a MinSalud Digital y transfirió la responsabilidad del Instituto Nacional de Salud al Ministerio de Salud. Junto con esta transferencia de responsabilidad, se produjo la transferencia de datos a la nueva autoridad. Por otra parte, en marzo de 2022, el gobierno sudafricano declaró su intención de ampliar el Sistema Electrónico de Datos de Vacunación (EVDS, por sus siglas en inglés) y "utilizarlo como posible plataforma de lanzamiento de un sistema portátil de registro sanitario". Estas medidas acarrean problemas de privacidad y protección de datos, ya que las personas que, inicialmente, se registraron para recibir una vacuna a través del EVDS o utilizaron la aplicación CoronApp para el rastreo de contactos, desconocían que sus datos personales podían estar vinculados a un sistema nacional de información sanitaria de mayor alcance.

Es probable que la transferencia de datos personales desde una plataforma cuyo único objetivo era rastrear los brotes de Covid-19 a un sistema diferente, que tiene un objetivo más amplio relativo a la salud nacional general, **viole el principio de finalidad**. Las leyes de protección de datos de muchos países exigen que los datos sólo se recopilen con fines específicos, explícitos y legítimos, y que no se procesen posteriormente de forma incompatible con dichos fines, especialmente cuando las personas no pueden elegir si quieren proporcionar sus datos.

El uso indebido de los datos recogidos con fines sanitarios de urgencia

También hemos observado que **algunos gobiernos han accedido a datos recopilados bajo la justificación de la salud pública y los han utilizado para fines diferentes, no relacionados con la salud**. En Australia, por ejemplo, la Comisionada de Información y Privacidad, Angelene Falk, halló pruebas que demuestran que la policía había accedido a historiales de registro de las aplicaciones móviles relacionadas con el Covid-19 sin una orden judicial para hacerlo, con el fin de facilitar sus investigaciones. En Hungría, funcionarios del gobierno tomaron las direcciones de correo electrónico que se utilizaban para registrarse a los fines de recibir las vacunas contra el Covid-19 y las utilizaron para marketing político directo en apoyo al actual Primer Ministro Viktor Orbán justo antes de las elecciones generales de 2022. En ambos casos, los datos que se recopilaron para gestionar la pandemia de Covid-19 se explotaron sin conocimiento ni consentimiento del usuario. En el caso de Australia, se infringieron las normas del procedimiento penal, así como la privacidad de los ciudadanos y residentes australianos; y, en el caso de Hungría, los datos se utilizaron indebidamente para tratar de influir en las elecciones a favor del gobierno de turno.

En resumen, nuestras principales preocupaciones relacionadas con la normalización de la vigilancia son las siguientes:

1. La readaptación indefinida, no especificada o poco clara de las tecnologías de vigilancia implementadas, originalmente, para luchar contra la propagación de la pandemia.
2. El uso de datos recopilados bajo el pretexto de luchar contra la propagación de la pandemia para fines ilegítimos y no relacionados con la emergencia ni con la salud.

CASO DE LA INDIA

Polémicas en torno a la nueva finalidad de la app de rastreo de contactos y su impacto en el derecho a la privacidad

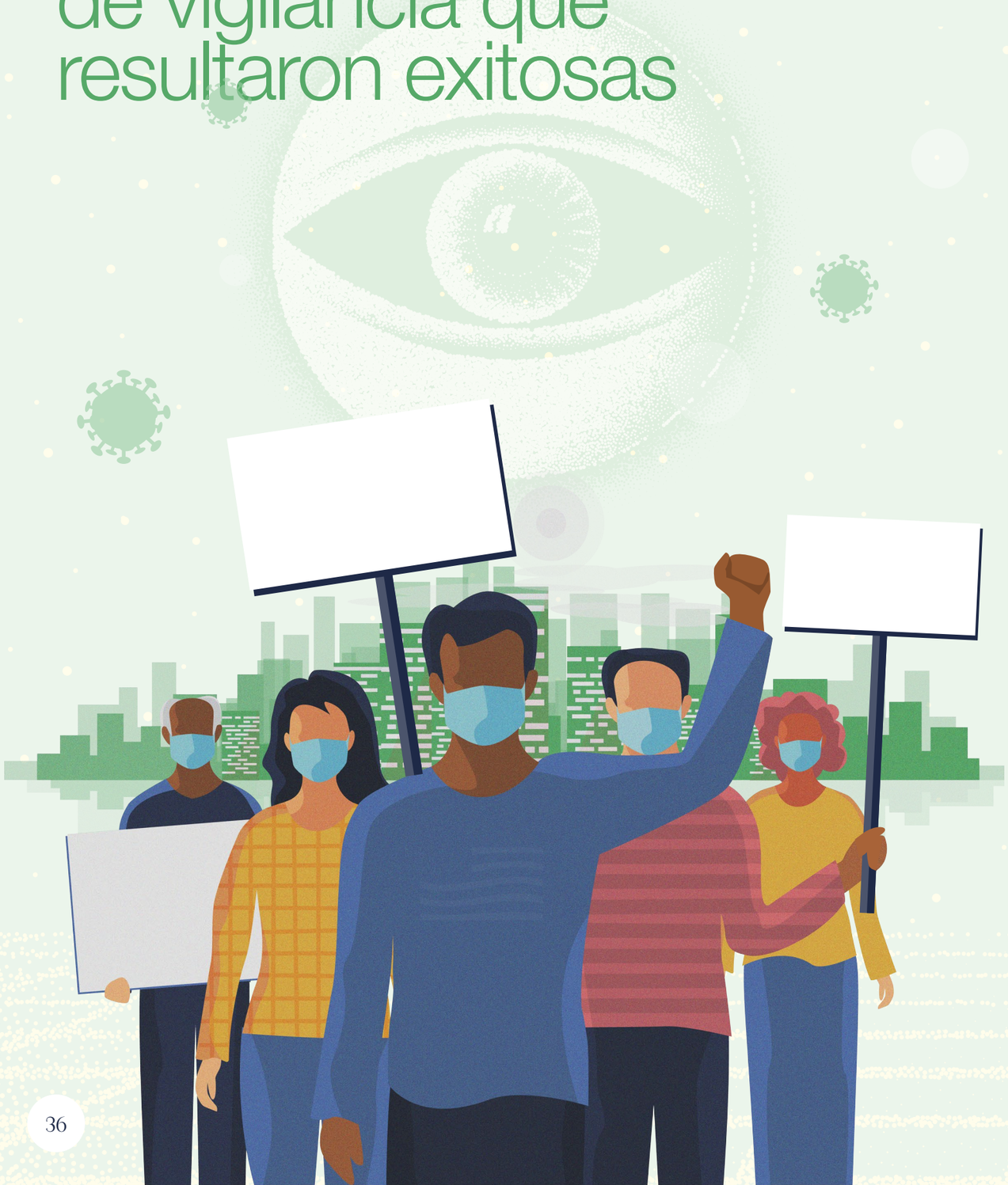
Informe de Amber Sinha

En julio de 2022, se anunció que el gobierno pretende convertir la aplicación de rastreo de contactos Aarogya Setu en una "aplicación nacional de salud", y no en una aplicación destinada únicamente a hacer frente a la pandemia de Covid-19. En el mismo sentido, el gobierno suspendió el protocolo de acceso e intercambio de datos de la aplicación, lo que generó serias dudas entre los activistas de la privacidad sobre el uso que se le daría a los datos. Previamente, el protocolo había establecido limitaciones sobre cómo Aarogya Setu podía gestionar y compartir los datos personales de la población; al ser discontinuado, comenzaron las preocupaciones sobre cómo la aplicación gestionaría los datos en el futuro, especialmente porque la finalidad de la aplicación también se estaba expandiendo.

Los usuarios no recibieron ninguna notificación de esta interrupción, que sólo salió a la luz en respuesta a una solicitud de liberar información presentada por la Internet Freedom Foundation en virtud de la Ley de Derecho a la Información de la India. La Internet Freedom Foundation también solicitó información sobre el destino de los datos recopilados durante la pandemia, pero el gobierno no dio una respuesta clara sobre si estos datos se habían eliminado, como se había anunciado en un principio. Esto confirmó los temores manifestados anteriormente por los activistas de la privacidad de que la aplicación se utilizaría para fines distintos a los relacionados con los servicios generales de salud nacional.

Actualmente, continúa habiendo incertidumbre sobre el estado de los datos recopilados por la aplicación. Cuando la Internet Freedom Foundation solicitó una actualización sobre la solicitud previa relativa al derecho a la información (para saber si los datos recopilados se habían eliminado) la respuesta del gobierno se limitó a redirigirlos a la política de privacidad de la aplicación. La política de privacidad establece que "al eliminar la aplicación se borrará toda la información recopilada y almacenada en su teléfono, pero no se eliminará la información almacenada en la nube. Si desea eliminar la información de registro mencionada en la cláusula 1(a) y almacenada en los servidores *backend*, puede cancelar su suscripción". Esto contradice la información publicada en la prensa, en la que se citaba la declaración de un funcionario anónimo de que todos los datos se habían eliminado de la aplicación y de los servidores públicos.

Acciones de la sociedad civil contra las medidas de vigilancia que resultaron exitosas



En el transcurso de la pandemia, las organizaciones de la sociedad civil han desempeñado un importante papel como organismos de fiscalización. Estamos en deuda con el trabajo que estas organizaciones han realizado para monitorear la crisis y documentar el impacto que las medidas de vigilancia relacionadas con el Covid-19 tuvieron sobre los derechos humanos y las libertades fundamentales. A continuación, mencionamos algunos ejemplos de campañas de litigio estratégico dirigidas por la sociedad civil para resistir la vigilancia ilegal a determinadas comunidades. Esta lista no es, en absoluto, exhaustiva; nuestra intención es compartir estas historias que resultaron exitosas para brindar herramientas que puedan resultar útiles a organizaciones de otros países.

La lucha contra los drones en Francia

En los primeros días de la pandemia, Francia decretó el confinamiento nacional y la policía de quince jurisdicciones utilizó cientos de drones para vigilar y hacer cumplir las órdenes de permanecer en casa. Los drones de la policía estaban equipados con cámaras y parlantes que emitían avisos indicando a la población que volviera a sus casas. En mayo de 2020, La Quadrature du Net (LQdN) y La Ligue des Droits de l'Homme presentaron una demanda para que se prohibiera el uso de drones utilizados para hacer cumplir el confinamiento impuesto por el Covid-19 en París. **Argumentaban que la policía no tenía fundamento jurídico para procesar los datos personales de los ciudadanos al grabarlos con drones.**

El Conseil d'État (el más alto tribunal administrativo de Francia) declaró que la policía de París infringía la Ley de Informática y Libertades del 6 de enero de 1978, que protege las libertades individuales en el tratamiento de los datos personales. La decisión emitida por el Conseil d'État estableció que era ilegal el hecho de que la policía utilizara drones equipados con cámaras a una altitud lo suficientemente baja como para que las personas pudieran ser identificadas a través de la ropa u otros signos distintivos. Sólo se concederían excepciones tras un decreto ministerial revisado por la autoridad francesa de protección de datos (CNIL). Aunque este caso se planteó por la vigilancia llevada a cabo durante la pandemia de Covid-19, su impacto fue más amplio, ya que la sentencia del Conseil d'État de marzo de 2020 también prohíbe el uso policial de drones para otros fines de investigación.

Acciones de la sociedad civil contra las medidas de vigilancia que resultaron exitosas

La victoria de LQdN, sin embargo, estuvo atravesada por numerosos desafíos. Entre mayo y octubre de 2020, la policía de París siguió utilizando drones para vigilar manifestaciones políticas. Alegaron que este uso era legal porque utilizaban una herramienta de inteligencia artificial para difuminar las grabaciones de los drones, aunque los medios de comunicación constataron que se podía eliminar el efecto difuminado de las imágenes "con facilidad." LQdN presentó otra denuncia contra la policía de París en octubre de 2020, alegando que la vigilancia con drones vulneraba las libertades civiles y la libertad de expresión. Volvieron a tener éxito y el Conseil d'État decretó que la policía de París debía "de forma inmediata, dejar de implementar medidas de vigilancia que utilizaran drones en reuniones públicas ." Esta decisión tiene implicancias aún más amplias que la sentencia de mayo de 2020 porque concluye que el uso de drones por parte de la policía es una cuestión de fondo y no sólo de procedimiento. LQdN sostiene que esta decisión limita seriamente la capacidad del gobierno francés para autorizar el uso de drones en los términos del artículo 22 de la nueva Ley de Seguridad Global, ya que ahora tendrán que demostrar que el uso de drones es de absoluta necesidad para garantizar la seguridad pública.

Esta victoria puso de manifiesto la necesidad de contar con fundamentos jurídicos claros y explícitos para estas herramientas de vigilancia. LQdN ha publicado el texto completo de sus reclamos judiciales en su página web, lo que permite que otros grupos utilicen esta argumentación para otros casos. Por ejemplo, en marzo de 2022, un grupo inspirado por LQdN presentó una denuncia ante el tribunal administrativo de Lyon y consiguió prohibir los helicópteros de vigilancia utilizados por la policía.

La defensa de las libertades fundamentales en Colombia

Como detallamos en la Tendencia nro. 3, el gobierno de Colombia lanzó una aplicación de rastreo de contactos, CoronApp, que recibió numerosas críticas de políticos y miembros de la sociedad civil por su falta de transparencia y rendición de cuentas. En noviembre de 2020, las autoridades aeroportuarias instaron, en reiteradas oportunidades, a un grupo de mujeres colombianas (Claudia Julieta Duque, Juanita Goebertus, Sol Marina de la Rosa y Alejandra Martínez), a descargarse la aplicación en sus teléfonos para poder embarcar en sus vuelos. Una de las mujeres, Claudia Julieta Duque, se negó y no le permitieron subir al avión. Duque es periodista y ha sido objeto de persecución por parte del Estado, por lo que le preocupaba, especialmente, que su privacidad pudiera verse comprometida.

Tras el incidente del aeropuerto, las mujeres iniciaron una acción de tutela de derechos fundamentales contra el Ministerio de Salud, el Instituto Nacional de la Salud y la Agencia de Regulación Aeroportuaria, solicitando al Tribunal Constitucional que interviniera y protegiera los derechos de las demandantes a la privacidad, protección de datos y libertad de circulación. Las mujeres alegaban que se habían vulnerado sus derechos fundamentales cuando se las obligó a descargar la CoronApp para poder viajar, y solicitaban al Tribunal que ordenara a las autoridades públicas que no hicieran obligatoria la aplicación. En particular, invocaron la protección del "derecho a conocer, actualizar y rectificar la información que hubiera sobre ellas en bancos de datos y en archivos de entidades públicas y privadas".

Las tres mujeres también recibieron el apoyo de grupos de la sociedad civil, como Fundación Karisma, AccessNow y Dejusticia, que presentaron memoriales en calidad de *amici curiae* ante el Tribunal Constitucional. AccessNow hizo hincapié en la importancia del consentimiento libre e informado y la provisión de alternativas para que las personas pudieran acceder a servicios clave sin utilizar la aplicación. Dejusticia cuestionó que la aplicación fuera realmente voluntaria, ya que miles de pasajeros se vieron obligados a descargarla para entrar o salir del país.

El litigio se demoró más de un año y la aplicación dejó de ser obligatoria en ese plazo. Finalmente, en abril de 2022, el Tribunal Constitucional analizó el caso y determinó que ya no existía riesgo de que sus derechos sean vulnerados porque la aplicación ya no era obligatoria. Sin embargo, al analizar el fondo del asunto, el Tribunal determinó que debía respetarse el derecho a la privacidad de las demandantes, incluso durante un estado de excepción nacional. Además, sostuvieron que las autoridades tenían el deber de "evitar el uso abusivo y arbitrario de los datos personales" y se ordenó a la Agencia Nacional Digital, al

Acciones de la sociedad civil contra las medidas de vigilancia que resultaron exitosas

INS y al Ministerio que respondieran a la petición de borrado de los datos de las demandantes. La acción de amparo planteada por Duque, Goebertus, de la Rosa y Martínez, y la posterior decisión del Tribunal Constitucional, tendrán, por lo tanto, importantes repercusiones en futuras crisis de salud pública y estados de excepción nacionales.

La resistencia a la vigilancia masiva en Israel

Como hemos descrito en la Tendencia nro. 1, al servicio nacional de inteligencia israelí, Shin Bet, se le ampliaron los poderes durante la pandemia, ya que se le otorgó la facultad de rastrear los movimientos de las personas a las que se había diagnosticado con Covid-19 y de las que podrían haberse infectado por proximidad. Estas medidas fueron introducidas como normas de emergencia por el poder ejecutivo y no estaban sujetas a supervisión parlamentaria.

El 18 de marzo de 2020, al día siguiente de que se anunciaran las medidas de emergencia, abogados de la Association for Civil Rights in Israel (ACRI) presentaron una petición al Tribunal Superior de Justicia, argumentando que el poder ejecutivo no debería poder eludir al parlamento y autorizar la vigilancia masiva. El 26 de abril, el Tribunal Superior de Justicia dictaminó que el Shin Bet "no estaba autorizado constitucionalmente a recopilar, procesar y utilizar 'información tecnológica'" de los pacientes de Covid-19. El Tribunal dictaminó que, sin aprobar una ley, el gobierno no estaba facultado para conceder poderes al Shin Bet para vigilar a la población bajo el pretexto de combatir la propagación del Covid-19.

En julio de 2020, el Parlamento aprobó una ley para autorizar temporalmente al Shin Bet a utilizar herramientas de vigilancia masiva para rastrear las infecciones por Covid-19 durante un periodo de seis meses. Ante esta situación, una coalición de grupos israelíes de defensa de los derechos humanos en Israel (ACRI, el Centro Adalah, Physicians for Human Rights - Israel, y Privacy Israel) presentó otra demanda ante el Tribunal Superior en septiembre de 2020 solicitando la derogación de la ley. En esta, afirmaban que el programa de vigilancia masiva del Shin Bet no era proporcional al objetivo de luchar contra el Covid-19, ya que atentaba contra las libertades fundamentales y el derecho a la privacidad. Además, alegaron que la ley recientemente aprobada era inconstitucional, ya que permitía utilizar una herramienta de seguridad nacional para fines civiles. En enero de 2021, el Tribunal Supremo dictaminó, finalmente, que "la amplia vigilancia viola gravemente los derechos humanos" y ordenó al gobierno que cesara el uso generalizado de la herramienta de rastreo del Shin Bet. Asimismo, estableció que, en el futuro, la herramienta sólo podría utilizarse en los casos en que las personas se negaran a cooperar con las investigaciones epidemiológicas.

En el transcurso de un año, la ACRI presentó media docena de peticiones al Tribunal Superior, algunas de las cuales fueron rechazadas y tuvieron que volver a presentarse. Al final, su tenacidad dio sus frutos. En cada petición, la ACRI incluía argumentos adicionales para reforzar su caso. Al principio, impugnaron la legalidad y constitucionalidad de las medidas de emergencia que eludían al Parlamento, y, más tarde, agregaron argumentos basados en la privacidad, la proporcionalidad y la eficacia.

Conclusión

La rápida implementación y readaptación de medidas y tecnologías de vigilancia para luchar contra la pandemia del Covid-19 han tenido efectos en los derechos humanos, las libertades fundamentales y el estado de derecho. En todo el mundo, los gobiernos desarrollaron y desplegaron herramientas -en muchos casos con una supervisión pública limitada- que violan el derecho a la privacidad de las personas y amenazan sus libertades civiles. Casi tres años después del inicio de la pandemia, parece que tanto los gobiernos y las organizaciones internacionales como las personas han pasado página, aceptando las medidas y prácticas de vigilancia que hemos analizado. Sin embargo, estas medidas y prácticas no deberían normalizarse teniendo en cuenta el efecto que tienen sobre nuestras libertades y democracias. Este es el momento de hacer un balance, evaluar la eficacia y proporcionalidad de las medidas y tecnologías de vigilancia implementadas para luchar contra la pandemia y determinar cuáles fueron las lecciones que se han aprendido para que los gobiernos y la sociedad civil estén mejor preparados para la próxima emergencia mundial.

Nuestra investigación nos ha permitido identificar cinco tendencias generales en las medidas de vigilancia relativas al Covid-19:

1. La readaptación de las medidas de seguridad existentes a nuevos fines

El sistema de lucha contra el terrorismo y las herramientas de vigilancia empleados por los servicios de inteligencia nacionales se transformaron para dar respuesta a la pandemia. Durante más de una década, los defensores de los derechos humanos han documentado cómo las leyes antiterroristas funcionan con escasa transparencia y limitada rendición de cuentas y se han utilizado para reprimir la disidencia y silenciar la crítica. Estas mismas preocupaciones surgen cuando los sistemas de lucha contra el terrorismo se aplican para dar respuesta a una pandemia. A modo de ejemplo, hallamos pruebas que demuestran que las leyes sobre ciberdelincuencia se ampliaron para censurar las voces críticas y perseguir a las personas acusadas de difundir información errónea sobre la pandemia en **Bangladesh, Indonesia, Kenia, Níger y Arabia Saudí**. La facilidad con la que se adaptaron los sistemas de lucha contra el terrorismo demuestra que cuando la definición de "terrorismo" es vaga, los Estados pueden instrumentalizarla para adoptar medidas represivas.

Libertad de expresión

Con el pretexto de combatir la desinformación sobre la pandemia de Covid-19, los gobiernos adaptaron las leyes sobre ciberdelincuencia a nuevos fines, introdujeron nuevas normas que penalizaban la difusión de "noticias falsas" y vigilaron la actividad en las redes sociales. Sin embargo, en países como **Camboya, Irán, India** y **Tailandia**, esto implicó un aumento de la vigilancia y la censura de periodistas y miembros de la sociedad civil, que se enfrentaron a sanciones penales, o a la eliminación de contenido cuando fueran acusados de difundir información falsa.

2. El silenciamiento de la sociedad civil

Con una motivación similar a la adaptación de las leyes sobre ciberdelincuencia, países como **Filipinas, Rusia y Sudáfrica** introdujeron nuevas leyes para penalizar la desinformación relacionada con la pandemia. Combinadas con penas desproporcionadas -hasta seis años de cárcel en Argentina- y criterios poco claros para definir lo que se considera desinformación, estas medidas contribuyen a crear un clima de miedo e intimidación, sobre todo en países en los que activistas y periodistas han sido históricamente blanco de ataques. Además, los Estados implementaron tecnologías como drones, robots patrulla y reconocimiento facial con el supuesto objetivo de hacer cumplir los confinamientos obligatorios, lo cual incrementó la vigilancia de los espacios públicos y se convirtió en una amenaza para la libertad de reunión. Es difícil medir el impacto total de las medidas de vigilancia que se implementaron para hacer frente a la pandemia de Covid-19 en el espacio cívico; es poco probable que alguien afirme que no asistió a una manifestación o que no expresó su opinión en las redes sociales por miedo a la vigilancia y a las represalias. Sin embargo, teniendo en consideración el contexto en el que se prohibieron las reuniones públicas y se dispersó por la fuerza a los manifestantes en, al menos, diez países de todo el mundo, podemos concluir que el "efecto disuasorio" de las tecnologías de vigilancia contribuye significativamente al silenciamiento de la sociedad civil.

Libertad de reunión

Algunas tecnologías de vigilancia, como drones, robots patrulla y reconocimiento facial, fueron desplegadas para vigilar los espacios públicos con el fin de hacer cumplir cuarentenas y confinamientos. Sin embargo, estas tecnologías pueden producir un efecto disuasorio sobre la voluntad de las personas para reunirse en público y expresar sus opiniones políticas. Esto sucede, en particular, cuando se las combina con otros fenómenos observados durante la pandemia, como la prohibición de protestas y grandes concentraciones, la aplicación irregular de las normas de distanciamiento social y el uso excesivo de la fuerza contra las personas que incumplían las órdenes de confinamiento.

3. El riesgo del uso indebido de datos personales

Los gobiernos implementaron diversas herramientas diseñadas para rastrear la propagación del virus, muchas de las cuales dependían de la recopilación de datos personales. Estas tecnologías se diseñaron e implementaron rápidamente, sin apenas consulta pública ni supervisión. Concluimos que muchas aplicaciones de rastreo de contactos no cumplían los principios fundamentales de protección de datos como la legalidad, la necesidad, la proporcionalidad y la minimización de datos. Por ejemplo, la Corte Constitucional de **Colombia** determinó, finalmente, que la recopilación de datos relacionada con el uso obligatorio de la aplicación de localización de contactos era ilegal. Por otro lado, encontramos pruebas que demuestran que en **Australia** y **Hungría** hubo funcionarios del gobierno que utilizaban datos de pacientes de Covid-19 para investigaciones policiales y marketing político directo, un claro uso indebido de datos que, originalmente, se habían obtenido para una finalidad específica. En general, las organizaciones locales de sociedad civil que realizaron estudios de casos observaron una falta de transparencia y rendición de cuentas en torno a las aplicaciones de rastreo de Covid-19. Esta opacidad hace que se torne difícil evaluar si la recopilación de datos fue proporcional a su carácter intrusivo y si se podrían haber alcanzado los mismos objetivos de salud pública por otros medios o con medidas alternativas que no resultaran violatorias de derechos.

Derecho a la privacidad

En muchos países, la respuesta a la pandemia se basó en la enorme recopilación de datos personales, incluidos datos sensibles, sin una justificación clara ni prueba de su proporcionalidad. La excesiva recopilación de datos vulneró el derecho a la privacidad, especialmente en países como **Israel** y **Pakistán**, donde las tecnologías de vigilancia masiva que originalmente habían sido diseñadas para luchar contra el terrorismo fueron utilizadas contra la ciudadanía. La recopilación invasiva e ilimitada de datos es especialmente preocupante para activistas y disidentes en países con un historial cuestionable en materia de derechos humanos.

Conclusión

4. El influyente papel de las empresas privadas

Además, hemos observado el influyente papel que desempeñaron las empresas privadas en la pandemia al cooperar con los gobiernos para desarrollar aplicaciones y herramientas de rastreo de contactos y participar en acuerdos de intercambio de datos. En países como **Colombia** y el **Reino Unido**, los gobiernos firmaron acuerdos poco claros de colaboración público-privada, cuyo alcance sólo se reveló luego de que activistas exigieran transparencia mediante el uso de las normas de acceso a la información pública. Esta falta de transparencia dificulta que la sociedad civil comprenda el alcance del intercambio de datos entre gobiernos y empresas privadas, evalúe el riesgo del uso indebido de datos y determine a quién responsabilizar en caso de violación de datos, como ocurrió en **Indonesia**.

La pandemia de Covid-19 fue uno de los primeros grandes acontecimientos sanitarios mundiales de la era de los *smartphones*, y, como tal, puso de manifiesto la creciente influencia de gigantes tecnológicos como Google y Apple. Debido a que estas empresas privadas controlan los sistemas operativos de los dispositivos móviles, pudieron crear los protocolos para las aplicaciones de rastreo de contactos y dar forma a las respuestas de salud pública, lo cual abrió muchos interrogantes sobre el rol que deben tener las empresas privadas, la supervisión democrática y la rendición de cuentas.

Libertad de circulación

El uso de herramientas de localización (como aplicaciones de rastreo de contactos, pulseras electrónicas y datos obtenidos a través de empresas de telecomunicaciones) permitió a los gobiernos rastrear la ubicación, los movimientos y las reuniones de las personas. Sin estas herramientas de vigilancia, los gobiernos habrían tenido menos posibilidades de implementar medidas excepcionales, tales como la imposición de confinamientos y cuarentenas obligatorios que vulneraban la libertad de circulación y limitaban la posibilidad de viajar dentro del país.

5. La normalización de la vigilancia más allá de la pandemia

Hacia finales de 2022, algunos gobiernos empezaron a retirar, gradualmente, las herramientas y medidas de vigilancia implementadas durante la pandemia, como el gobierno de Canadá, que anunció su plan de sacar de servicio su aplicación de Covid-19 para el rastreo de contactos en junio de 2022. Celebramos estos esfuerzos. Sin embargo, hemos observado que, en otros países, la vigilancia estatal continúa y ha sido normalizada. En este informe, hemos descrito cómo los Estados reutilizaron leyes y tecnologías antiterroristas y las aplicaron a civiles en nombre de la lucha contra el Covid-19. Actualmente, debemos tener cuidado con el fenómeno opuesto: la normalización y adaptación de las medidas y herramientas utilizadas durante el Covid-19. Tenemos razones suficientes para pensar que existe la posibilidad de que ocurra una readaptación de medidas/herramientas para servir a nuevos objetivos, pues ya hemos visto a algunos gobiernos anunciar su intención de utilizar los datos recopilados durante la pandemia para fines secundarios (como el desarrollo de plataformas nacionales de salud en **Colombia**, **India** y **Sudáfrica**). A primera vista, este cambio que va de Covid-19 a la salud pública general puede parecer poco problemático. Sin embargo, el uso de datos recogidos, originalmente, en circunstancias excepcionales para fines que no son de emergencia viola el principio de limitación de la finalidad y contribuye a la normalización de un estado de vigilancia que acumula grandes cantidades de datos personales de forma intrusiva y desproporcionada con respecto a su necesidad.

Recomendaciones

Resumen

Basándonos en las conclusiones, elaboramos recomendaciones detalladas para los Estados, las empresas y la sociedad civil. Estas recomendaciones reflejan los debates con una comunidad más amplia de actores civiles, incluidos los participantes de un taller organizado durante el Foro para la Gobernanza de Internet de 2022 en Addis Abeba (Etiopía).

Nuestras recomendaciones a los Estados se centran en la necesidad de llevar a cabo una revisión seria de las tecnologías de vigilancia utilizadas durante la pandemia de Covid-19 y de extraer lecciones de esta experiencia para futuras crisis. En primer lugar, los Estados deberían subsanar el desarrollo apresurado y poco claro de las herramientas de vigilancia y realizar una evaluación cuidadosa de su impacto en los derechos humanos. Deberían poner fin a las medidas que no cumplan las normas de derechos humanos o que ya no sean necesarias para dar respuesta a la pandemia.

En segundo lugar, dado que nuestros asociados que trabajan en terreno tienen, generalmente, dificultades para obtener información incluso básica (como el fundamento jurídico o la situación actual de una medida de vigilancia), creemos que existe una necesidad urgente de que los Estados se comprometan a adoptar medidas de transparencia, incluida la difusión constante de leyes, reglamentos, información orientativa, así como de políticas. En las recomendaciones detalladas a continuación, esbozamos la cantidad mínima de información que debería hacerse pública.

En tercer lugar, los Estados deberían examinar las leyes y políticas introducidas o aplicadas durante la pandemia y evaluar su conformidad con las normas internacionales de derechos humanos. Este proceso debería llevarse a cabo en público y en diálogo con las partes interesadas, incluida la sociedad civil, y debería conducir al desarrollo de garantías claras de los derechos humanos para el uso de herramientas de vigilancia en futuras emergencias. Estas garantías deberían ser coherentes con el derecho internacional de los derechos humanos y deberían traducirse en leyes y procedimientos. A continuación, detallamos los elementos clave de estas propuestas, incluidas las garantías de protección de datos y las cláusulas de caducidad para evitar la readaptación a nuevos fines de las medidas de emergencia.

Teniendo en cuenta **el influyente papel de las empresas privadas en el diseño y despliegue de respuestas tecnológicas a la pandemia**, creemos que es urgente mejorar en términos de transparencia estas asociaciones con organismos estatales, pero también las propias prácticas de las empresas, especialmente en lo que se refiere a la protección de datos. Instamos a las empresas a que revisen sus tecnologías desde una perspectiva de derechos humanos y que dejen de desarrollar y vender aquellas que no cumplan las normas internacionales, incluidas las leyes de protección de datos. Las empresas también deberían poner en marcha políticas y procedimientos de derechos humanos que guíen el desarrollo de la tecnología para futuras emergencias y establezcan cómo piensan responder a las solicitudes gubernamentales de acceso a los datos.

Por último, consideramos que la s**ociedad civil desempeña un papel importante** a la hora de supervisar las respuestas de los Estados a las emergencias y las prácticas de las empresas privadas, y de evaluarlas desde el punto de vista de los derechos humanos. Como demuestran los casos mencionados de litigios e incidencia que resultaron exitosos, la presión civil es necesaria para promover el debate público sobre las tecnologías y las medidas de vigilancia, así como para que los Estados y las empresas privadas rindan cuentas.

Recomendaciones detalladas

Para los agentes estatales

Revisión de las medidas y leyes de vigilancia

- **Revisar** todas las medidas, tecnologías y sistemas de vigilancia implementados para hacer frente a la pandemia de Covid-19 a fin de evaluar su compatibilidad con los derechos humanos y el impacto que tuvieron en ellos, incluidos los marcos jurídicos de protección de datos.
- Luego de realizar la evaluación, **dejar de utilizar** las tecnologías y medidas de vigilancia que sean incompatibles con las normas internacionales de derechos humanos y la legislación aplicable
- **Eliminar** los datos personales y **desactivar** las aplicaciones que ya no sean necesarias.
- Revisar públicamente la compatibilidad de las **leyes y las políticas nacionales** que se aplicaron durante la pandemia con la legislación internacional sobre derechos humanos y los regímenes de protección de datos.
- Brindar soluciones legales para cada una de las violaciones de derechos humanos identificadas.

Transparencia sobre las medidas de vigilancia durante la pandemia de Covid-19

Hacer públicos, como mínimo, los siguientes puntos:

- Todas las medidas, tecnologías y sistemas de vigilancia utilizados desde el inicio de la pandemia; si se siguen utilizando y por qué.
- Las especificaciones técnicas de todas las aplicaciones, sistemas y dispositivos utilizados durante la pandemia, independientemente de si se han ido eliminando gradualmente.
- Todas las asociaciones público-privadas, incluidos los acuerdos y la documentación pertinente, que se hayan realizado desde el inicio de la pandemia, así como las asociaciones existentes a las que se recurrió durante la pandemia.
- Los resultados de cualquier revisión que se haya realizado, incluidas las evaluaciones de impacto sobre los derechos humanos y las revisiones de eficacia y cómo informaron sobre los procesos de toma de decisiones.
- Los registros de tratamiento de datos, incluidas las evaluaciones de impacto sobre la protección de datos, información sobre los tipos de datos recopilados y con qué fines, qué partes tuvieron acceso, cuánto tiempo se almacenarán o si fueron eliminados, y cómo se garantizaron los derechos de los interesados.

Garantías para el uso de medidas de vigilancia en futuras emergencias

- **Revisar** y/o desarrollar marcos jurídicos y procedimientos que regulen las medidas y tecnologías de vigilancia, así como el papel del sector privado, para garantizar que cumplen las normas internacionales de derechos humanos.

  Todas las leyes y políticas que regulen los poderes de vigilancia en contextos de emergencia deben exigir lo siguiente a los organismos estatales:
  - ◊ Realizar y publicar evaluaciones de impacto sobre los derechos humanos, incluidas evaluaciones de impacto sobre la protección de datos, de cada medida o tecnología de vigilancia.
  - ◊ Aportar pruebas de que cada medida o tecnología cumple las normas de derechos humanos. Definir un proceso de revisión periódica para evaluar su eficacia y cumplimiento.

Recomendaciones

- ◊ Establecer garantías de protección de datos que incluyan, como mínimo, lo siguiente: un fundamento jurídico claro y adecuado; una finalidad limitada y específica para el tratamiento de datos personales y la limitación del tratamiento sólo a los datos que sean necesarios para este fin; periodos de conservación de datos claramente definidos y una "cláusula de caducidad" para todas las medidas o tecnologías; respeto de los derechos de las personas, incluido el acceso a la información y soluciones legales.
- ◊ Establecer mecanismos de supervisión adecuados y eficaces.
- ◊ Abstenerse de readaptar medidas y herramientas a nuevos fines.

- Garantizar **una participación y consulta públicas serias** durante el proceso de diseño, desarrollo, despliegue, actualización y revisión de las medidas o tecnologías de vigilancia. En particular, crear comités de supervisión en los que participen todas las partes interesadas, incluidos tecnólogos, la sociedad civil, la academia y miembros de las comunidades más afectadas por las medidas adoptadas, para revisar periódicamente las herramientas implementadas.
- Garantizar que las medidas, herramientas y leyes de vigilancia, incluidas las adoptadas en situaciones de emergencia, **no se utilicen para reprimir la disidencia o la participación ciudadana**.
- Garantizar que las medidas, herramientas y leyes de vigilancia no den lugar a que los movimientos, comportamientos y/o estado de salud de las personas se utilicen con fines lucrativos y/o comerciales.
- Prohibir la vigilancia biométrica general e indiscriminada en los espacios públicos.

Para las empresas

- **Revisar las tecnologías y los sistemas** desplegados durante la pandemia de Covid-19 para garantizar que éstos cumplen las normas internacionales de derechos humanos, incluidos los Principios Rectores sobre las Empresas y los Derechos Humanos de la ONU, y las leyes nacionales.
- **Dejar de realizar** cualquier actividad que tenga impactos negativos sobre los derechos humanos o tomar las medidas necesarias para mitigar dichos impactos.
- **Adoptar políticas de derechos humanos** que se apliquen a las actividades del sector empresarial, incluidos procedimientos para evaluar las solicitudes gubernamentales de acceso a datos de forma que, en la medida de lo posible, se garantice el cumplimiento de las normas internacionales de derechos humanos.
- Publicar, y poner directamente a disposición de las personas afectadas, información sobre las actividades de tratamiento de datos, las medidas establecidas para proteger los datos personales y los mecanismos de reclamación existentes.
- Publicar informes de transparencia en los que se describan los casos en los que se han solicitado y compartido datos de usuarios con organismos estatales, los tipos de datos (incluidos los metadatos) solicitados y compartidos, el número total de solicitudes y la tasa de cumplimiento.
- Publicar información sobre colaboraciones público-privadas con organismos estatales. Incluir, como mínimo, la naturaleza y los fines de la colaboración, su duración, información sobre el tratamiento de datos personales y los derechos de las personas afectadas.
- Garantizar el acceso a una reparación adecuada cuando las acciones de la empresa hayan tenido consecuencias negativas o hayan contribuido a generarlas.

Recomendaciones

Para la sociedad civil

- Supervisar e investigar las medidas de vigilancia relativas al Covid-19 que tomaron los gobiernos y su grado de cumplimiento de las normas internacionales de derechos humanos, así como de las leyes locales y regionales, en particular las de protección de datos. Si procede, buscar vías de comunicación y jurídicas para impugnar estas medidas.
- Mantenerse alerta ante la posibilidad de que se readapten herramientas para servir a objetivos distintos de los originales. Instar a los gobiernos a introducir y respetar cláusulas de caducidad que se comprometan a eliminar los datos y desmantelar los sistemas de vigilancia apenas dejen de ser estrictamente necesarios.
- **Exigir transparencia a los organismos estatales sobre:**
  - ◊ Planes a largo plazo relativos a los datos recopilados en el marco de la respuesta a la pandemia de Covid-19, con el fin de que aclaren su uso, almacenamiento y reutilización de los mismos.
  - ◊ Acuerdos de intercambio de datos entre organismos estatales, incluidos los organismos supranacionales.
  - ◊ Acuerdos de intercambio de datos entre los sectores público y privado.
  - ◊ Pruebas demostrables de la eficacia de las herramientas y medidas de vigilancia.
  - ◊ Revisiones periódicas del impacto sobre las comunidades que resultaron más afectadas por las herramientas y medidas de vigilancia.
- Abogar por la revisión o el desarrollo de legislación y políticas adecuadas para futuras crisis sanitarias y otras emergencias, y exigir que la sociedad civil sea consultada en este proceso.
- Presionar a las empresas para que rindan cuentas por las consecuencias negativas que causen sus actividades en los derechos humanos.

Quiénes somos

Este informe es el resultado de un esfuerzo conjunto del European Center for Not-for-Profit Law, la International Network of Civil Liberties Organizations y algunos de sus miembros, y Privacy International, con el apoyo de Nina Dewi Toft Djanegara en la investigación y la edición.

Los miembros del **European Center for Not-for-Profit Law Stichting (ECNL)** tienen más de 20 años de experiencia tanto en la creación como en la defensa de entornos jurídicos y políticos más favorables para grupos civiles, movimientos y activistas. Creamos conocimiento y trabajamos con aliados para establecer normas universales y regionales que protejan y amplíen las libertades civiles, tanto en el ámbito cibernético como fuera de él. Nos centramos en los factores que afectan a estas libertades a nivel mundial y en las complejas necesidades de la sociedad civil, incluida la necesidad de optimizar las garantías de los derechos fundamentales en el desarrollo y funcionamiento de la tecnología, y los sistemas y dispositivos de inteligencia artificial (IA). Con respecto al abordaje del impacto de la tecnología en el espacio cívico, tendemos puentes entre los responsables políticos, académicos y la industria, por un lado, y las organizaciones de la sociedad civil que no se dedican a los derechos digitales, incluidos los representantes de grupos marginados y vulnerables. Hemos establecido, conjuntamente, redes temáticas de la sociedad civil (por ejemplo, sobre seguimiento de protestas, lucha antiterrorista, IA) y desarrollado herramientas de seguimiento del espacio cívico (por ejemplo, Covid-19 Civic Freedoms Tracker). Asimismo, nos dedicamos a la defensa de leyes y políticas mundiales, regionales y nacionales relacionadas con la Inteligencia Artificial y las tecnologías emergentes, incluida la Ley de Inteligencia Artificial de la UE y el convenio marco sobre Inteligencia Artificial del Consejo de Europa. ECNL es miembro del Global Internet Forum to Counter-Terrorism, del Financial Action Task Force Private Consultantive Forum, afiliado a la European Digital Rights Initiative (EDRi), y representante de la Conferencia de Organizaciones No Gubernamentales Internacionales (CINGO, por sus siglas en inglés) en el Comité del Consejo de Europa sobre Inteligencia Artificial.

Quiénes somos

La **International Network of Civil Liberties Organizations (INCLO)** es una red formada por 15 organizaciones nacionales independientes de derechos humanos de distintos países del norte y del sur que trabajan en conjunto para promover los derechos y las libertades fundamentales. INCLO apoya y refuerza mutuamente el trabajo de las organizaciones miembros en sus respectivos países y colabora de manera bilateral y multilateral. INCLO entiende que las organizaciones miembros son más fuertes juntas, capaces de ayudar a la consecución de logros que perduren en el tiempo, potenciar el éxito de las demás y compartir conocimientos, habilidades y recursos. Los miembros de la INCLO tienen décadas de experiencia en la consecución de significativos cambios sociales en todo el mundo, gracias a su profundo conocimiento del panorama jurídico, político y cultural de quince países. Los miembros de la INCLO empoderan a las personas para que se apropien de su futuro y construyan el futuro que necesitamos para que todos puedan vivir con seguridad y libertad tal y como son. Las conclusiones de este informe cuentan con el respaldo general de los miembros de INCLO, Agora, la Association for Civil Rights in Israel, la Canadian Civil Liberties Association, el Centro de Estudios Legales y Sociales de Argentina, la Hungarian Civil Liberties Union, el Human Rights Law Centre de Australia, el Irish Council for Civil Liberties y Liberty del Reino Unido.[2]

Privacy International (PI) es una organización no gubernamental sin fines de lucro con sede en Londres (número de organización benéfica: 1147471) que trabaja con asociados a nivel mundial para abogar por soluciones jurídicas y tecnológicas que protejan a las personas, y a sus datos, de la explotación por parte de gobiernos y empresas. Expone daños y abusos, moviliza a aliados en todo el mundo, realiza campañas con el público para encontrar soluciones, y presiona a empresas y gobiernos para que cambien. PI se enfrenta a la excesiva vigilancia estatal y empresarial para que las personas de todo el mundo puedan disfrutar de una mayor seguridad y libertad gracias a una mayor privacidad personal. En el marco de sus actividades, PI investiga cómo se generan y explotan los datos personales y cómo pueden protegerse mediante marcos jurídicos y tecnológicos.

La investigación para los estudios de casos nacionales fue realizada por socios del proyecto en 6 países: Colombia (Dejusticia), Francia (La Quadrature du Net), India (Amber Sinha), Indonesia (KontraS), Kenia (Comisión Nacional de Derechos Humanos de Kenia) y Sudáfrica (Legal Resources Centre). Los socios locales recibieron una lista de preguntas para orientar su trabajo de investigación. Los estudios de caso incluidos en este informe fueron redactados por las organizaciones aliadas, con comentarios editoriales de ECNL, INCLO y PI.

El **Centro de Estudios de Derecho, Justicia y Sociedad (Dejusticia)** es un centro de estudios jurídicos y sociales dedicado a fortalecer el Estado de Derecho y promover los derechos humanos en Colombia y el sur global. Promueve el cambio social a través de estudios rigurosos y de sólidas propuestas de políticas públicas, y realiza campañas de incidencia en foros de alto impacto. También lleva a cabo litigios estratégicos y diseña e imparte programas educativos y de formación.

La Quadrature du Net (LQDN) promueve y defiende las libertades fundamentales en el mundo digital. LQDN lucha contra la censura y la vigilancia, tanto de Estados como de empresas privadas. Cuestionan cómo el mundo digital y la sociedad se influyen mutuamente, y trabajan por una Internet que sea libre, descentralizada y empoderante.

Amber Sinha es un investigador independiente que trabaja en la intersección entre el derecho, la tecnología y la sociedad, y estudia el impacto de las tecnologías digitales en los procesos y estructuras sociopolíticas. Su investigación tiene como objetivo impulsar el discurso sobre las prácticas reguladoras en torno a internet, la tecnología y la sociedad. Hasta junio de 2022 fue Director Ejecutivo del **Centre for Internet and Society, India**, donde dirigió programas sobre privacidad, gobernanza de datos, IA e identidad. En la actualidad, es Investigador Principal de IA fiable en Mozilla Foundation, donde estudia modelos de transparencia algorítmica. El primer libro de Amber, The Networked Public, fue publicado en 2019. Estudió Derecho y Humanidades en la National Law School de India University, Bangalore.

[2] Aunque el informe no analiza la situación en Estados Unidos, la American Civil Liberties Union respalda las principales recomendaciones formuladas en él.

Quiénes somos

KontraS, la comisión para los desaparecidos y las víctimas de violencia, es una organización no gubernamental nacional de derechos humanos con sede en Yakarta, Indonesia. Sus principales actividades están orientadas a apoyar a las víctimas de violaciones de derechos humanos. Busca incrementar el respeto y la protección de los derechos humanos en Indonesia mediante actividades de defensa, investigación, campañas y presión política. KontraS se centra en diversos temas, como las desapariciones forzadas, la tortura, la impunidad y las violaciones de los derechos civiles, políticos, económicos, sociales y culturales.

La Comisión Nacional de Derechos Humanos de Kenya (**Kenya Human Rights Commission - KHRC**) es una institución líder no gubernamental de derechos humanos y gobernanza en África, fundada en 1992 con la misión de fomentar los derechos humanos, los valores democráticos, la dignidad humana y la justicia social. Se ocupa de cuestiones y situaciones relacionadas con los derechos humanos y la justicia social a todos los niveles de la sociedad. Las intervenciones de la KHRC se ejecutan en el marco de cuatro objetivos estratégicos y programas temáticos interdependientes: Derechos Civiles y Políticos; Derechos Económicos y Sociales; Igualdad y No Discriminación, y Desarrollo Institucional y Sostenibilidad. La KHRC es reconocida por su larga trayectoria, tenacidad, coherencia, experiencia y pasión a la hora de proporcionar liderazgo técnico y político a programas relevantes de derechos humanos y gobernanza a todos los niveles.

El **Legal Resources Centre** (**LRC**) es una clínica jurídica sudafricana de interés público y sin fines de lucro fundada en 1979. Desde su creación, el LRC se ha comprometido a trabajar por una sociedad plenamente democrática basada en el respeto del Estado de Derecho y la democracia constitucional. El LRC utiliza el derecho como herramienta legal para facilitarle a las personas vulnerables y marginadas la reivindicación y el desarrollo de sus derechos; promover la igualdad de género y racial, y resistir todas las formas injustas de discriminación; así como contribuir al desarrollo de la jurisprudencia en materia de derechos humanos, y a la transformación social y económica de la sociedad.

Agradecimientos:

Nina Dewi Toft Djanegara (Universidad de Stanford), Karolina Iwańska, Katerina Hadzi Miceva Evans, Andrea Judit Toth, Emily Lawton (ECNL), Olga Cronin, Lucila Santos, Elizabeth Farries, Myriam Selhi (INCLO), Ilia Siatitsa (Privacy International).

Daniel Ospina Celis, Lucía Camacho, Juan Carlos Upegui (Dejusticia), Bastien Le Querrec (La Quadrature du Net), Amber Sinha (Policy), Nadine Sherani, Rozy Sodik, Auliya Rayyan (KontraS), Martin Mavenjina (Kenya Human Rights Commission), Sherylle Dass, Devon Turner (Legal Resources Centre).

También agradecemos a Ivana Rosenzweigova por su contribución al proyecto y a Taryn McKay por el diseño gráfico.

Diciembre de 2022

European Center for Not-for-Profit Law

INCLO INTERNATIONAL NETWORK OF CIVIL LIBERTIES ORGANIZATIONS

PRIVACY INTERNATIONAL