Naciones Unidas A/75/147

Asamblea General

Distr. general
27 de julio de 2020
Español
Original: inglés

**Septuagésimo quinto período de sesiones**
Tema 72 b) del programa provisional*
**Promoción y protección de los derechos humanos: cuestiones de derechos humanos, incluidos otros medios de mejorar el goce efectivo de los derechos humanos y las libertades fundamentales**

# Derecho a la privacidad

## Nota del Secretario General

El Secretario General tiene el honor de transmitir a la Asamblea General el informe preparado por el Relator Especial del Consejo de Derechos Humanos sobre el derecho a la privacidad, Joseph A. Cannataci, presentado de conformidad con la resolución 28/16 del Consejo.

* A/75/150.

20-10082 (S) 110920 170920

# Informe del Relator Especial sobre el derecho a la privacidad, Joseph A. Cannataci

*Resumen*

En el presente informe, el Relator Especial sobre el derecho a la privacidad, Joseph A. Cannataci, propone una evaluación preliminar de los efectos de la pandemia de enfermedad por coronavirus (COVID-19) en la privacidad. Todavía no se dispone de la base empírica necesaria para determinar de manera concluyente si las medidas contra la COVID-19 que afectan la privacidad son necesarias y proporcionadas en una sociedad democrática. El Relator Especial examina dos aspectos particulares de las repercusiones de la COVID-19 en el derecho a la privacidad: la protección de datos y la vigilancia.

Las actividades de vigilancia y de rastreo de contactos relacionadas con la COVID-19 pueden adoptar diversas formas y pueden ser manuales o tecnológicas, anónimas o no, y consensuadas o no. Las inquietudes surgen cuando se propone o se despliega apresuradamente un aparato de vigilancia tradicionalmente empleado para fines de seguridad del Estado con el propósito de rastrear datos relacionados con la salud en beneficio de la salud pública en el contexto de una pandemia.

Si un Estado determina que es preciso aplicar medidas de vigilancia tecnológica como respuesta a la pandemia mundial de COVID-19, debe asegurarse, tras demostrar tanto la necesidad como la proporcionalidad de las medidas específicas, de disponer de una ley que prevea tales medidas explícitamente. La ley debe incluir salvaguardias que, si no se explican con suficiente detalle, no pueden considerarse adecuadas en virtud del derecho internacional.

Está previsto publicar un informe más definitivo sobre el tema en 2021, cuando se dispondrá de más pruebas que permitirán realizar una evaluación más precisa.

# I. Introducción

1. Los efectos de la pandemia de enfermedad por coronavirus (COVID-19) en la privacidad constituyen un tema apropiado y oportuno para el presente informe a la Asamblea General, dado que los derechos humanos, incluido el derecho a la privacidad, sufren efectos serios y, en general, negativos a causa de la pandemia. De hecho, las respuestas que están configuradas en función de los derechos humanos y los respetan son más idóneas para vencer la pandemia, garantizar la atención de la salud para todos y preservar la dignidad humana[1].

2. Si bien la prioridad es salvar vidas, la lucha contra la COVID-19 y el respeto de los derechos humanos, incluido el derecho a la privacidad, no son incompatibles. Por ejemplo, la seguridad de los ciudadanos de que se tiene en cuenta su privacidad fomenta la confianza y la voluntad de apoyar proactivamente las medidas adoptadas por el Estado para prevenir la propagación del virus. Los derechos humanos pueden dotar a los Estados de la capacidad de ganarse la confianza de sus ciudadanos.

3. El presente informe constituye una evaluación preliminar, ya que todavía no se dispone de la base empírica necesaria para determinar de manera concluyente si las medidas contra la COVID-19 que afectan la privacidad son necesarias y proporcionadas en una sociedad democrática. Está previsto publicar un informe más definitivo a mediados de 2021, cuando se dispondrá de 16 meses de pruebas que permitirán realizar una evaluación más precisa.

4. En el informe, el Relator Especial aborda dos aspectos particulares de las repercusiones de la COVID-19 en el derecho a la privacidad: la protección de datos y la vigilancia. Sin embargo, reconoce que hay muchas más cuestiones de privacidad en juego durante la pandemia, incluidas las relativas a los niños, el género y el papel que desempeñan los algoritmos, entre otras.

**Aspectos destacados**

5. Las inquietudes sobre la privacidad planteadas por la COVID-19 no surgieron en un vacío, sino que se manifestaron en un entorno en el que ya existían problemas de privacidad que estaba abordando el Relator Especial sobre el derecho a la privacidad, como la vigilancia y la protección adecuada de los datos relacionados con la salud.

6. Si bien la pandemia de COVID-19 ha generado un gran debate sobre el valor del rastreo de contactos y la dependencia de la tecnología que permite hacer un seguimiento de los ciudadanos y las personas con quienes se encuentran, el uso de la información y la tecnología no es nuevo en la gestión de las emergencias de salud pública. Lo que resulta preocupante en algunos Estados son los informes sobre la forma en que se utiliza la tecnología y el grado de intromisión y control al que se somete a los ciudadanos, posiblemente con escaso efecto en la salud pública.

7. La COVID-19 es una enfermedad y, en tanto cuestión sanitaria, cabe mencionar lo siguiente:

a) Las leyes de varios Estados relativas a la salud pública prevén desde hace tiempo medidas que pueden adoptarse para combatir enfermedades transmisibles, y que proporcionan una norma con respecto a la cual deben examinarse las medidas específicas contra la COVID-19;

[1] Naciones Unidas, “COVID-19 y los derechos humanos: en esto estamos todos juntos”, informe de políticas, abril de 2020.

b) El contexto necesario para considerar la información personal y sobre la salud en la pandemia de COVID-19 debe entenderse en el marco del enfoque general de la sociedad para tratar los datos relacionados con la salud.

8. Las medidas aplicadas en nombre de la lucha contra la COVID-19 que afectan la privacidad, incluidas las actividades de vigilancia, no pueden ni deben considerarse fuera de contexto, sino que deberían examinarse como parte de una política global e integral que rija la vigilancia en los respectivos Estados, y en consonancia con ella.

9. En cuanto al uso de la tecnología moderna para controlar la propagación de la pandemia, en general, no se ha dado la debida importancia a la subdisciplina de la ingeniería de la privacidad.

10. En las recomendaciones formuladas anteriormente por el Relator Especial, en particular las relativas a las actividades de vigilancia realizadas por los organismos del Estado (A/HRC/37/62) y a la protección de la privacidad de los datos relacionados con la salud (A/74/277)[2], se ofrecen directrices para ayudar a los Estados a hacer frente a la pandemia de COVID-19 sin dejar de respetar sus obligaciones en virtud del derecho internacional de los derechos humanos.

# II. Protección de los datos y actividades de vigilancia durante la pandemia de COVID-19

11. Resulta útil examinar brevemente las medidas ordinarias de salud pública anteriores a la COVID-19 relativas a las enfermedades transmisibles y de declaración obligatoria.

12. Las leyes y procedimientos que rigen las enfermedades transmisibles existen desde hace siglos e incluyen estrictas medidas de cuarentena, así como hospitales de cuarentena, para contrarrestar pandemias como la de peste bubónica. Más recientemente, se observó en el Reino Unido de Gran Bretaña e Irlanda del Norte un ejemplo del papel de los Estados en la implementación de respuestas y procesos de salud pública. Durante la mayor parte de dos siglos, tras la labor de John Snow sobre el brote de cólera de Broad Street de 1854 y la mayor comprensión del riesgo que plantean las enfermedades transmitidas por el agua, el perfil de la salud pública en el Reino Unido comenzó a cambiar. En 1939 se introdujo un sistema de inspectores sanitarios en el Reino Unido, en partes del Imperio británico y en otros lugares. Los inspectores de salud a nivel local se aseguraban de que se cumplieran las leyes de saneamiento, desde las conexiones de alcantarillado hasta las instalaciones para lavarse las manos en las tiendas. Ya estaban en la primera línea contra enfermedades transmisibles como el cólera y la tuberculosis antes del estallido de la Segunda Guerra Mundial, que provocó situaciones en las que esas enfermedades podían propagarse más fácilmente, especialmente condiciones de alojamiento insalubres y abarrotadas. Los inspectores de salud eran por lo general funcionarios públicos especialmente capacitados que tenían —y siguen teniendo— normas estrictas de notificación y presentación de informes para asegurar que los médicos del departamento de salud pública fueran alertados de los brotes de enfermedades infecciosas graves. Los médicos tomaban luego medidas para contener y erradicar esas enfermedades.

13. Por consiguiente, la dimensión jurídica de la evolución de las medidas de salud pública incluía la comunicación obligatoria de información a las autoridades de salud

[2] Pueden consultarse los apéndices conexos y un memorando explicativo de esos informes (incluidas versiones amplias sin editar) en www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx.

pública de que se había detectado un determinado tipo de enfermedad. Eso se conoce como una enfermedad de declaración obligatoria.

14. La COVID-19 es una enfermedad de declaración obligatoria. En un Estado Miembro, figura en el número 66 de la lista de enfermedades de ese tipo. Por lo tanto, ya se habían identificado 65 enfermedades sobre las que se había notificado a las autoridades nacionales de salud pública.

15. La transferencia de datos personales delicados mediante la notificación de una enfermedad transmisible es una medida ordinaria a nivel nacional, pero también tiene una dimensión internacional. Aunque no es extraordinaria, la transferencia de esos datos puede dar lugar a situaciones en las que se invocan medidas extraordinarias.

16. Una vez notificada la incidencia de una enfermedad, las autoridades de salud pública disponen por ley de un arsenal de opciones y medidas, que van desde adoptar una actitud de espera hasta la más estricta de las cuarentenas. En otras palabras, una vez que reciben datos sanitarios sobre un paciente determinado, se espera que las autoridades de salud pública tomen una decisión informada sobre lo que deben hacer.

17. En la mayoría de los países desarrollados, los datos personales relacionados con la salud se tratan de manera confidencial y se procesan según las necesidades, lo que incluye el almacenamiento con fines epidemiológicos. Uno de los principales objetivos de las autoridades de salud pública es utilizar la epidemiología para prevenir y combatir las epidemias. Lo vienen haciendo, generalmente con buenos resultados, incluso desde antes de la era de los teléfonos inteligentes y la COVID-19. De hecho, hay cada vez más pruebas de que, en la mayoría de los países desarrollados que adoptaron medidas sensatas de manera oportuna, a mediados de julio de 2020, la COVID-19 se había combatido con éxito, e incluso contenido, utilizando metodologías tradicionales sin recurrir a las tecnologías relacionadas con los teléfonos inteligentes[3].

18. El rastreo de contactos es la herramienta clásica empleada por las entidades de salud pública para detener la propagación de enfermedades transmisibles. Constituye una intromisión en la vida privada porque requiere que el paciente revele con quién ha estado en contacto durante un período de tiempo determinado. Tradicionalmente, en la mayoría de los países, este ha sido de manera implícita uno de los casos excepcionales en que el derecho a la privacidad no tiene por qué ser absoluto. La necesidad de detener la propagación de una posible epidemia constituye uno de los poquísimos casos de bien común en los que el interés público se valora socialmente por encima del derecho a la privacidad o, incluso, de otros derechos como la libertad de circulación y la libertad de asociación. En pocas palabras, para evitar la propagación del cólera o la tuberculosis, por ejemplo, las autoridades tienen derecho a: a) saber quién sufre la enfermedad y b) ordenar el aislamiento estricto bajo normas sanitarias estrictas, entre otras cosas.

19. Todas las pruebas disponibles indican que actualmente no hay ninguna alternativa al rastreo de contactos ni un sustituto razonable que permita detener, limitar y, a menudo, contener el contagio. No hay duda de que, siempre que sea factible, el rastreo de contactos funciona satisfactoriamente y que, aunque afecta la privacidad de las personas, puede clasificarse como una medida necesaria.

20. Los procedimientos de rastreo de contactos manuales y rigurosos que afectan la privacidad también pueden entenderse adecuadamente como proporcionados en función de la necesidad de prevenir, contener o combatir de otra manera un peligro

[3] Véanse, por ejemplo, los casos de Grecia y Malta; si el principal criterio o medida del éxito o el fracaso fuera el número de muertes por millón de habitantes, estos países podrían considerarse ejemplos de manejo exitoso del virus sin vigilancia tecnológica.

para la salud pública, como una epidemia. La naturaleza y la cantidad de información personal requerida y normalmente recogida en las actividades de rastreo de contactos es la estrictamente necesaria para detener la propagación de la enfermedad tratando de dilucidar quién podría haber sido infectado. Entonces, por ejemplo, el depósito más completo de información privada del paciente, a saber, su teléfono inteligente, no se secuestra en el curso del rastreo de contactos tradicional, así como tampoco se accede a él. Las autoridades sanitarias, a menudo acompañadas por agentes de policía que aplican la ley sanitaria pertinente, llaman por teléfono o visitan personalmente a quienes pueden haber estado en contacto con la persona infectada y hacen cumplir el curso de acción prescrito, que a menudo es el aislamiento voluntario durante un tiempo determinado.

21. Las facultades de registro e incautación están ligadas desde hace mucho tiempo al derecho a la privacidad. En algunos países la salud pública es un asunto de interés público considerado tan primordial que las facultades de registro e incautación ordinarias (no extraordinarias) de las autoridades de salud pública suelen ser mayores que las de la policía. Rara vez aparecen casos del uso de esas facultades en las noticias, y se observa claramente la presunción a favor de la salud pública. Así pues, en algunos Estados, si bien el registro de locales por la policía requiere a menudo una orden judicial o ejecutiva, no ocurre lo mismo si el registro se realiza en virtud de una ley de salud pública, aunque el funcionario de salud pueda estar acompañado por un agente de policía durante dicho registro.

## A. Medidas extraordinarias

22. En la mayoría de los Estados, la legislación pertinente otorga a las autoridades de salud pública la facultad de adoptar medidas extraordinarias. Esto ocurre normalmente en el contexto de una emergencia de salud pública, que puede ser nacional o localizada, y que debe ser declarada formalmente para que se puedan invocar medidas extraordinarias. Una “emergencia de salud pública” suele definirse vagamente, si es que se define, y en algunos países la ley estipula que la jefatura de la autoridad de salud pública tiene la potestad de decidir qué situación constituye una emergencia de ese tipo. Se puede encontrar orientación, por ejemplo, en las definiciones de la Organización Mundial de la Salud (OMS).

23. Las facultades relacionadas con las emergencias sanitarias son enormes y pueden, literalmente, incluir cualquier acción imaginable (véase el apartado g)) que sea “necesaria para reducir, eliminar o suprimir la amenaza para la salud pública”[4]. La autoridad de salud pública puede:

a) Segregar o aislar a cualquier persona en cualquier zona;

b) Evacuar a cualquier persona de cualquier zona;

c) Impedir el acceso a cualquier zona;

d) Controlar la circulación de cualquier vehículo;

e) Ordenar que cualquier persona se someta a un examen médico;

f) Ordenar que cualquier sustancia u objeto sea incautado, destruido o eliminado;

g) Ordenar que se tome cualquier otra medida que considere apropiada.

24. Cuando un Estado otorga a sus autoridades de salud pública facultades tan amplias en caso de una emergencia de salud pública, se plantea la cuestión de si el

[4] Malta, Ley de Salud Pública, capítulo 465 de la legislación de Malta, art. 15.

acceso regular o constante al dispositivo de una persona, como un teléfono inteligente, o la vigilancia del paradero y los contactos de una persona por medio de la geolocalización de un teléfono inteligente es una medida necesaria y proporcionada.

25. Esto también se aplica en contextos en los que algunos Estados no han esperado a que exista una emergencia de salud pública antes de brindar fundamentos jurídicos para acceder al dispositivo de una persona. De hecho, en algunos países, tal acceso es una facultad ordinaria (no extraordinaria) de las autoridades sanitarias, que pueden "inspeccionar, extraer o incautar cualquier registro o hacer una copia de cualquier registro pertinente para la salud pública, cualquiera que sea la forma en que se mantenga y, cuando se mantenga cualquier registro por medio de una computadora:

> i) Tendrán acceso a cualquier computadora, cualquier aparato o material asociado que sea o haya sido o pueda haber sido utilizado en relación con los registros, e inspeccionarán y comprobarán su funcionamiento;
>
> ii) Exigirán a toda persona que tenga a su cargo la computadora, el aparato o el material, o que se ocupe de su funcionamiento, que les preste la asistencia que razonablemente necesiten"[5].

26. Podría afirmarse que esas disposiciones tienen por objeto proporcionar acceso puntual en una situación normal y no a una escala que involucre grandes porcentajes o toda la población de un Estado, como se ha contemplado, ensayado o realizado durante la crisis de la COVID-19 hasta la fecha.

## B. Normativa sobre la privacidad y los datos relacionados con la salud

27. Los datos relacionados con la COVID-19 son datos de salud, que constituyen la primera categoría de datos personales que califica para gozar de niveles especiales de protección. Se puede decir que la protección de los datos relacionados con la salud es la pionera de las normas y reglamentos en materia de protección de datos. El juramento hipocrático, que dataría de entre los siglos VI y III a. C., exige a los médicos preservar el secreto y la confidencialidad de la información médica de sus pacientes[6].

28. Toda situación médica genera inevitablemente datos personales que requieren ser procesados según las más altas normas jurídicas y éticas. El debate sobre la privacidad que surgió en los Estados Unidos de América en 1973 incluyó los primeros principios para el manejo de los datos relacionados con la salud, mientras que en Europa, la primera recomendación del Consejo de Europa sobre protección de datos, formulada en 1980, se refería a los datos médicos y fue anterior a que se celebrara el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio 108), de enero de 1981. Desde entonces, la recomendación del Consejo se ha revisado dos veces (en 1997 y en 2019).

29. La digitalización de los datos ha dado lugar a un importante crecimiento del volumen de datos relacionados con la salud que se procesan y ha permitido contar con perfiles más completos de los pacientes. No solo permitió aumentar la calidad de los datos, sino que también ha facilitado el intercambio de información entre los

[5] *Ibid.*, art. 6 1) c).

[6] Institute of Medicine, *Health Data in the Information Age: Use, Disclosure, and Privacy* (Washington D. C., National Academies Press, 1994).

profesionales de la salud, incrementando así las posibilidades de mejorar la prestación de servicios sanitarios.

30. La persona a la que se refieren los datos tiene un interés manifiesto en los datos y en controlarlos. Los parientes de esa persona, los terceros que mantienen relaciones transaccionales con ella y otros interesados indirectos, como la comunidad de la persona, el público en general y los investigadores médicos, también tienen interés en esos datos. Los intereses son diversos, variados y desiguales, por lo que se amerita contar con distintas disposiciones específicas para garantizar el merecido respeto del derecho a la privacidad, de conformidad con el artículo 12 de la Declaración Universal de Derechos Humanos.

31. El conjunto de interesados indirectos que muestran interés por los datos relacionados con la salud ha crecido exponencialmente en los últimos tiempos, y ese crecimiento se refleja igualmente en las tensiones entre los diferentes interesados, lo que da lugar a cuestiones jurídicas y éticas cada vez más difíciles.

32. Tanto el Reglamento General de Protección de Datos[7] de la Unión Europea como el Convenio 108[8] del Consejo de Europa reconocen los datos sobre la salud como una "categoría especial de datos". En virtud del Convenio, el procesamiento de datos relacionados con la salud solo es permisible cuando la ley consagra salvaguardias apropiadas. Si bien el Reglamento prevé más situaciones en las que se pueden procesar datos relacionados con la salud, el procesamiento de los datos de ese tipo sigue estando sujeto a mayores restricciones que el de los datos personales más genéricos. El Reglamento permite a los Estados miembros de la Unión Europea "mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud"[9].

33. En marzo de 2019, el Comité de Ministros del Consejo de Europa adoptó la Recomendación CM/Rec(2019)2, relativa a la protección de los datos relacionados con la salud[10]. La recomendación contiene una serie de principios destinados a proteger los datos relacionados con la salud, que incorporan tanto las disposiciones del Convenio 108 como las adiciones introducidas en el Convenio Modernizado para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal de 2018, conocido como el Convenio 108+, que tenían por objeto garantizar que el Convenio respondiera a los nuevos desafíos de la era digital[11].

34. En octubre de 2019, el Relator Especial presentó oficialmente a la Asamblea General la Recomendación sobre la protección y el uso de los datos relacionados con la salud (A/74/277, anexo). En la Recomendación se reconoce el carácter delicado y el alto valor comercial de los datos relacionados con la salud, y se establece una base de referencia internacional común para las normas mínimas de protección de esos datos[12]. La Recomendación tiene por objeto complementar los reglamentos y recomendaciones existentes, teniendo en cuenta al mismo tiempo el creciente

[7] Unión Europea, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), 2016, art. 9 1).

[8] Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio 108), 1981, art. 6.

[9] Unión Europea, Reglamento General de Protección de Datos, art. 9 4).

[10] Véase https://edoc.coe.int/en/international-law/7969-protection-of-health-related-date-recommendation-cmrec20192.html.

[11] Consejo de Europa, "Protection of health-related data: Council of Europe issues new guidelines", comunicado de prensa (marzo de 2019). Puede consultarse en www.coe.int/en/web/portal/-/health-related-data-council-of-europe-issues-new-guidelines.

[12] A/74/277, anexo, párr. 4.1 c).

procesamiento digitalizado de los datos sobre la salud de las personas. Se abordan las lagunas y las incertidumbres que se produjeron con la introducción de los historiales médicos electrónicos, las aplicaciones móviles, las actividades de promoción orientadas a grupos concretos, el acceso de empleadores y compañías de seguros a los datos relacionados con la salud, y las necesidades de protección de datos que son particulares de grupos específicos de la sociedad, como las personas con discapacidad y los refugiados.

35. La Recomendación es prueba de cómo han evolucionado las salvaguardias de protección de datos a lo largo del tiempo para mantenerse al día con los avances de la sociedad y la tecnología. Cada vez que han surgido crisis internacionales, en especial las ocasionadas por pandemias mundiales, se han puesto a prueba las normas y recomendaciones existentes. Las razones de salud pública siempre han proporcionado, y siguen proporcionando, un fundamento jurídico legítimo para el procesamiento de datos personales y datos relacionados con la salud, con el fin de combatir y contener la propagación de una pandemia. En la Recomendación se especifica que el tratamiento de datos relacionados con la salud es legítimo cuando se realiza en aras del interés público y con las debidas salvaguardias, especialmente medidas adecuadas en materia de seguridad y organización[13].

36. Los datos relativos a la salud de las personas se han convertido en un instrumento clave utilizado por Gobiernos y científicos de todo el mundo en la lucha contra la propagación incesante de la COVID-19. Varios Gobiernos, y a menudo sus respectivas fuerzas de seguridad, están procesando datos de ese tipo (a veces asociándolos con otros metadatos[14] personales, como datos de localización) con miras, entre otras cosas, a hacer cumplir las obligaciones de cuarentena o de aislamiento voluntario, o a alimentar las investigaciones encaminadas a configurar las medidas restrictivas necesarias en materia de interacción social. En algunos casos, las entidades que tienen acceso a esos datos personales delicados son interesados indirectos nuevos, cuya repentina aparición puede haberse producido a expensas de políticas coherentes que salvaguarden la privacidad y la integridad de los datos relacionados con la salud.

37. Una de las formas en que los Gobiernos y las empresas de tecnología están procesando los datos relacionados con la salud en la lucha contra la pandemia de COVID-19 es utilizando la tecnología para hacer un seguimiento de las personas que dieron positivo en las pruebas de la enfermedad y, por extensión, de todas las personas con las que puedan haber estado en contacto. Esta extensión tecnológica del proceso tradicional de rastreo de contactos se realiza a menudo mediante el procesamiento de datos generados por los teléfonos móviles, y es un enfoque que se ha probado en el control de crisis pandémicas anteriores, por ejemplo, en 2014, en los esfuerzos contra la propagación del virus del Ébola en África Occidental, y en 2015, en la lucha contra el síndrome respiratorio de Oriente Medio (MERS)[15]. Hoy más que nunca, y especialmente a la luz del uso más generalizado de la telefonía móvil, este método de rastreo de contactos tiene el potencial de permitir a los Gobiernos y a sus respectivas autoridades de salud pública controlar con éxito el riesgo que plantean las pandemias, como la de COVID-19, así como vigilar la propagación y la evolución a largo plazo

[13] *Ibid.*, párr. 4.1 f).

[14] Privacy International define los metadatos como cualquier conjunto de datos que describa y proporcione información sobre otros datos, como la fecha y hora de un mensaje electrónico, el nombre del remitente, el nombre de un destinatario y la ubicación del dispositivo, entre otros. Véase “Extraordinary powers need extraordinary protection”, 20 de marzo de 2020. Puede consultarse en https://privacyinternational.org/news-analysis/3461/extraordinary-powers-need-extraordinary-protections.

[15] Privacy International, “Extraordinary powers need extraordinary protections”, 20 de marzo de 2020.

de una enfermedad. El procesamiento de los datos relativos a la salud de las personas merece la elaboración de una reglamentación apropiada, basada en la Recomendación del Relator Especial sobre la protección y el uso de los datos relacionados con la salud, y que debería consagrarse en la legislación nacional de los Estados.

38. La Recomendación ofrece la orientación necesaria a los Estados que opten por legislar para el procesamiento seguro de los datos relacionados con la salud, incluso en los escenarios mundiales sin precedentes que plantea la COVID-19. Todos los interesados indirectos están incluidos en el ámbito de la Recomendación, ya que su aplicabilidad no se limita a los profesionales médicos y de la salud, sino que abarca el "procesamiento de los datos relacionados con la salud en todos los sectores de la sociedad, incluidos los ámbitos público y privado"[16]. Exige que todos los responsables y los encargados del procesamiento adopten todas las medidas apropiadas para cumplir sus obligaciones con respecto a los datos relacionados con la salud, y que puedan demostrar a una autoridad supervisora competente que el procesamiento de datos se está llevando a cabo teniendo en cuenta todas las obligaciones aplicables[17]. Ese requisito se hace eco además del llamamiento a los Estados para que establezcan autoridades de supervisión independientes que estén en condiciones de controlar la implementación de las actividades de vigilancia necesarias, incluidas aquellas orientadas a la epidemiología, como se explicará más adelante. Un recuento muy aproximado realizado por el titular del mandato sugiere que, en el mejor de los casos, menos de 60 Estados cumplen parcialmente las normas mínimas establecidas en la Recomendación. Dicho de otro modo, más del 70 % de los Estados Miembros de las Naciones Unidas están muy lejos de cumplir esas normas. Por lo tanto, una pregunta clave que debe hacerse un ciudadano preocupado es: ¿en qué medida, si es que lo hace, aplica efectivamente mi país las normas establecidas en la Recomendación sobre la protección y el uso de los datos relacionados con la salud?

39. Cabe señalar que el Convenio 108+ exige que, "incluso en situaciones particularmente difíciles, se respeten los principios de protección de datos"[18]. Es importante tener presente que los Estados tienen el deber de proteger la salud de sus ciudadanos, pero también de proteger por igual su derecho a la privacidad, tanto en las medidas adoptadas a corto plazo como en la planificación a largo plazo. Ambos deberes no se contradicen entre sí y se alienta a los Estados a que consulten la Recomendación como marco para las normas y legislación que serían necesarias para brindar el fundamento jurídico apropiado para el procesamiento de los datos relacionados con la salud, incluso cuando ello pueda entrañar, con carácter excepcional, actividades de vigilancia.

40. Un año después de la presentación oficial de la Recomendación a la Asamblea General, y en medio de una crisis sanitaria como la de la COVID-19, es necesario adoptar medidas urgentes para subsanar los actuales niveles bajos de cumplimiento de las normas establecidas en la Recomendación.

[16] A/74/277, anexo, párr. 2.1.

[17] *Ibid.*, párr. 4.5.

[18] Consejo de Europa, "Joint Statement on the right to data protection in the context of the COVID-19 pandemic by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe", 30 de marzo de 2020. Puede consultarse en https://rm.coe.int/covid19-joint-statement/16809e09f4.

## C. La vigilancia y los datos relacionados con la salud

### Vigilancia por parte de los organismos de cumplimiento de la ley, inteligencia y seguridad

41. El mandato del Relator Especial sobre el derecho a la privacidad se creó en 2015 en respuesta directa a las revelaciones de Edward Snowden sobre las actividades de vigilancia realizadas por organismos del Estado. Tras más de dos años de amplias consultas, en marzo de 2018 el Relator Especial presentó al Consejo de Derechos Humanos un proyecto de instrumento jurídico[19] sobre las actividades de vigilancia llevadas a cabo por las fuerzas del orden y los servicios de seguridad e inteligencia.

42. En el documento se esbozan muchos de los principios básicos y las medidas mínimas (salvaguardias y recursos) que un Estado debe respetar o introducir para cumplir con el artículo 11 de la Declaración Universal de Derechos Humanos y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos. Como han señalado importantes tribunales regionales[20], las actividades de vigilancia en la sociedad moderna son permisibles siempre que estén previstas en la ley y sean necesarias y proporcionadas en una sociedad democrática. Si se llevan a cabo actividades de ese tipo, debe quedar claro que la salvaguardia clave es la supervisión eficiente y oportuna de dicha vigilancia.

43. Entre las normas mínimas recomendadas como esenciales figura la existencia de una autoridad independiente encargada de supervisar *ex ante* y *ex post* todas las medidas de vigilancia adoptadas tanto por las fuerzas del orden como por los servicios de inteligencia. Por consiguiente, el derecho interno de todos y cada uno de los Estados debería consagrar una supervisión eficaz tanto de los organismos encargados de hacer cumplir la ley como de los servicios de seguridad e inteligencia, por parte de autoridades de supervisión independientes y dotadas de recursos adecuados. Como confirma la jurisprudencia del Tribunal Europeo de Derechos Humanos y del Tribunal de Justicia de la Unión Europea, la vigilancia debe ser selectiva si es posible y realizarse siempre de manera adecuada, con la autorización previa de una autoridad externa independiente, preferiblemente, pero no necesariamente, integrada por al menos una persona de rango judicial.

44. La gran mayoría de los Estados están muy lejos de cumplir esas normas. En julio de 2020, de los 193 Estados Miembros de las Naciones Unidas, solo una pequeña minoría (menos del 10 %) estaba cerca de cumplir las normas necesarias para que un Gobierno asegure la protección y el respeto adecuados de la privacidad de los ciudadanos en lo que respecta a las actividades de vigilancia realizadas por organismos del Estado.

45. El panorama relativo a la COVID-19 se complica aún más cuando se proponen o se despliegan apresuradamente aparatos de vigilancia tradicionalmente empleados para fines de seguridad del Estado con un propósito de salud pública, como la lucha contra la COVID-19.

46. Para proteger a las personas de la injerencia en su derecho a la privacidad, los Gobiernos deben estar sujetos a procedimientos reglamentarios previstos en la legislación nacional. Los Estados deberían incluir en sus leyes medidas cautelares destinadas a garantizar que no se puedan iniciar actividades de vigilancia hasta que,

[19] Véase el proyecto de instrumento jurídico sobre vigilancia gubernamental y privacidad. Puede consultarse en www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.pdf.

[20] Véase Tribunal Europeo de Derechos Humanos, *Big Brother Watch and Others v. the United Kingdom* (solicitudes núms. 58170/13, 62322/14 y 24960/15), sentencia de 13 de septiembre de 2018.

o a menos que, se demuestre a una autoridad independiente y competente que dicha vigilancia es legal, necesaria y proporcionada respecto del objetivo que se persigue, es decir, "con el único fin de asegurar el reconocimiento y el respeto de los derechos y libertades de los demás, y de satisfacer las justas exigencias de la moral, del orden público y del bienestar general en una sociedad democrática"[21].

47. El Relator Especial ha recomendado también que los Estados complementen esas medidas incorporando en su ordenamiento jurídico interno las normas y salvaguardias establecidas en el Convenio 108+, especialmente en el artículo 11, y que toda información personal que intercambien los servicios de inteligencia y las fuerzas de seguridad dentro y fuera de las fronteras esté sujeta a la supervisión de sus autoridades nacionales independientes.

48. Se alienta a todos los Estados a que introduzcan en su ordenamiento jurídico interno una ley detallada sobre las actividades de vigilancia realizadas por las fuerzas del orden y los servicios de seguridad e inteligencia con salvaguardias de supervisión, o bien que actualicen las leyes vigentes, a fin de proporcionar el fundamento jurídico para medidas de vigilancia que sean necesarias y proporcionadas en una sociedad democrática, y en pleno cumplimiento del artículo 9 del Convenio 108 y el artículo 11 del Convenio 108+. El Relator Especial ha procurado fomentar una mayor conciencia e intercambio de buenas prácticas en materia de supervisión de la vigilancia con la creación del Foro Internacional de Supervisión de los Servicios de Inteligencia, que se viene reuniendo anualmente desde 2016. Se insta a los Estados a que interactúen con sus pares y participen activamente en el Foro.

**La vigilancia en el contexto de la epidemiología: una herramienta para luchar contra la propagación de enfermedades**

49. Durante sus estudios, los estudiantes de epidemiología, a diferencia de los abogados especializados en cuestiones de privacidad, aprenden que la vigilancia se define como "el escrutinio continuo de todos los aspectos de la aparición y propagación de una enfermedad que son pertinentes para un control eficaz" y que implica "tareas sistemáticas de reunión, análisis, interpretación y difusión de datos sobre la salud". La detección y el diagnóstico de enfermedades es "el acto de descubrir una enfermedad o una instancia de enfermedad nueva, emergente o reemergente e identificar su causa". El diagnóstico es "la piedra angular de los esfuerzos eficaces de control y prevención de enfermedades, incluida la vigilancia"[22].

50. La vigilancia en el contexto de la epidemiología siempre se ha considerado clave para controlar eficazmente la propagación de una enfermedad. Esa vigilancia incluye información relativa a datos médicos, como diagnósticos clínicos, tasas de mortalidad y otra información pertinente necesaria para detectar y rastrear la enfermedad, en cuanto a las personas, los lugares, y las fechas y horas. Ese enfoque[23] se reforzó particularmente con la propagación del VIH/sida, la hepatitis C y la fiebre hemorrágica del dengue.

51. Dado que todos los países desempeñan un papel en la propagación de las epidemias, los marcos jurídicos de cada país establecen sistemas nacionales de

[21] Declaración Universal de Derechos Humanos, art. 29 2).

[22] Institute of Medicine, *Global Infectious Disease Surveillance and Detection: Assessing the Challenges–Finding Solutions, Workshop Summary* (Washington D. C., National Academies Press, 2007).

[23] La pandemia de "gripe española" de 1918-1919, que según las estimaciones causó la muerte de unos 40 millones de personas en todo el mundo, hizo evidente la necesidad de una vigilancia eficaz de la salud pública destinada a detectar y prevenir las pandemias de ese tipo.

presentación de informes relativos a la propagación de enfermedades infecciosas, por lo general, de la manera que se señaló anteriormente.

52. La OMS tiene el mandato de dirigir y coordinar la vigilancia mundial para la presentación de esos informes. El Reglamento Sanitario Internacional (2005) constituye un acuerdo jurídicamente vinculante con 196 países, entre los que se encuentran todos los Estados miembros de la OMS y algunos Estados no miembros. Los Estados signatarios están obligados a informar de cualquier evento que pueda constituir "una emergencia de salud pública de importancia internacional". Una emergencia de esas características se define como "un evento extraordinario que [...] se ha determinado que: i) constituye un riesgo para la salud pública de otros Estados a causa de la propagación internacional de una enfermedad, y ii) podría exigir una respuesta internacional coordinada".

53. Por consiguiente, el requisito de notificación amplio tiene un alcance que trasciende las enfermedades transmisibles o de declaración obligatoria, y tiene por objeto específico la detección temprana y satisfactoria de todos los sucesos de salud pública que puedan tener graves consecuencias internacionales. En particular, el Reglamento reconoce enfermedades específicas que se consideran especialmente preocupantes y obliga a los signatarios a informar inmediatamente a la OMS de cualquier caso concreto de determinadas enfermedades, entre ellas el síndrome respiratorio agudo severo (SRAS), independientemente del contexto en que se produzca.

54. El intercambio de datos de la OMS durante una emergencia de salud pública "permite realizar análisis para comprender lo más plenamente posible la emergencia, con miras a asegurar que las decisiones se basen en las mejores pruebas disponibles". Distintas disposiciones se aplican a cada una de las tres categorías siguientes:

a) Vigilancia, epidemiología y respuesta en casos de emergencia, incluidos los centros de salud;

b) Secuencias genéticas;

c) Estudios de observación y ensayos clínicos[24].

55. Se alienta a los Estados partes en el Reglamento Sanitario Internacional a que compartan datos con el fin de prevenir la propagación de cualquier pandemia mundial, y la OMS se compromete a publicar únicamente datos anonimizados. Esos datos publicados incluirían datos obtenidos de las actividades de vigilancia y control, comunicados por los Estados parte, así como datos relativos a la respuesta de emergencia del Estado respectivo. Un ejemplo de esa respuesta sería el rastreo de contactos y los detalles relativos al tratamiento. Los datos publicados también pueden incluir información sobre los centros médicos, como su ubicación y los recursos de los que disponen. El artículo 45 del Reglamento establece los requisitos de protección de esos datos, incluida la eliminación de cualquier dato personal y relacionado con la ubicación.

56. En el informe de la OMS sobre la vigilancia mundial de las enfermedades infecciosas con tendencia epidémica se enumeran los tipos de datos de vigilancia que se suelen reunir y notificar con respecto a las enfermedades infecciosas. Uno de los métodos de vigilancia informa sobre la confirmación de los casos observados en los servicios de salud. Esto se conoce como vigilancia pasiva, ya que equivale a informar de casos que no se han investigado activamente. Otro método es la vigilancia de las cepas de la enfermedad. En el caso de algunas enfermedades, como la gripe, aparecen con frecuencia nuevas cepas. Otro informe es el generado por la detección en la

[24] OMS, "Policy statement on data sharing by the World Health Organization in the context of public health emergencies", 13 de abril de 2016.

población, que consiste en examinar activa y sistemáticamente a la población para encontrar casos de la enfermedad en la comunidad.

57. Por consiguiente, las prácticas de vigilancia, control y rastreo de contactos no son conceptos nuevos en la recolección de información con fines epidemiológicos. La OMS hace referencia a esas medidas con miras a proteger a las poblaciones de la propagación de cualquier epidemia.

58. La OMS enumera los siguientes objetivos de la labor de vigilancia en el contexto de la COVID-19:

a) Permitir la rápida detección, el aislamiento, las pruebas y el manejo de los presuntos casos;

b) Rastrear a los contactos y hacer un seguimiento;

c) Orientar la aplicación de las medidas de control;

d) Detectar y contener los brotes en poblaciones vulnerables;

e) Evaluar el impacto de la pandemia en los sistemas de atención de la salud y en la sociedad;

f) Vigilar las tendencias epidemiológicas a largo plazo y la evolución del virus de la COVID-19;

g) Comprender la cocirculación del virus de la COVID-19, el de la gripe y otros virus respiratorios[25].

59. Los objetivos enumerados anteriormente podrían justificarse en el marco de la salud pública o el interés público, y es probable que constituyan una razón jurídica y justificable para procesar datos relativos a la salud, pero solo en la medida en que se procesen de conformidad con la legislación de protección de datos promulgada en consonancia con la Recomendación del Relator Especial sobre la protección y el uso de los datos relacionados con la salud.

60. La vigilancia con fines epidemiológicos, descrita anteriormente, puede adoptar muchas formas, pero debe ser necesaria y proporcionada en función de los objetivos que se pretende alcanzar. Los objetivos mencionados podrían utilizarse como guía para que los Estados determinen sus propios objetivos.

## D. La tecnología y los datos relacionados con la salud: consideraciones de privacidad y salud pública

### Fundamento jurídico de las medidas ordinarias y extraordinarias y necesidad de respuestas proporcionadas y mesuradas

61. Como se mencionó anteriormente, los tratados internacionales y la mayoría de las Constituciones nacionales contienen disposiciones que permiten a los Estados incrementar transitoriamente sus facultades durante un período de crisis. Los Gobiernos pueden hacer uso de facultades excepcionales, que en circunstancias normales se considerarían vulneraciones o violaciones de los derechos humanos y las libertades fundamentales, durante un tiempo limitado y con un propósito específico, que normalmente es combatir o prevenir una amenaza inminente (en este caso, prevenir la propagación de la COVID-19).

[25] OMS, “Surveillance strategies for COVID-19 human infection”, Coronavirus (COVID-19) update núm. 29, 5 de junio de 2020.

62. Los Estados tienen diversas maneras de hacer uso de las facultades ampliadas, según lo dispuesto en su Constitución o en los tratados internacionales ratificados. Algunos pueden llamarlo “estado de emergencia”, otros, “estado de necesidad”, mientras que, especialmente durante la actual crisis de la COVID-19, otros han declarado una “emergencia de salud pública”. Cada régimen jurídico especial de carácter temporal otorga diferentes facultades a las autoridades. Por ejemplo, las investigaciones realizadas hasta la fecha indican que al menos 15 Estados del Norte Global[26] han declarado el estado de emergencia en respuesta a la crisis actual.

63. En una declaración[27] emitida al principio de la crisis, un grupo de expertos de los procedimientos especiales subrayó la importancia de que los Estados encuentren el equilibrio adecuado entre las medidas extraordinarias adoptadas para luchar contra la propagación de la COVID-19 y la protección de los derechos humanos. Las medidas extraordinarias están —o deberían estar— estrictamente definidas en las leyes y Constituciones nacionales como órdenes legales de forma específica emitidas por las autoridades dotadas de facultades excepcionales en un estado de emergencia. También están reconocidas en instrumentos jurídicos internacionales, entre ellos el Pacto Internacional de Derechos Civiles y Políticos (art. 4) y el Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales (art. 15)[28].

64. La importancia de coordinar adecuadamente las medidas adoptadas para evitar el contagio a gran escala de la COVID-19 con el respeto de los derechos humanos fundamentales, incluido el derecho a la protección de datos, se aborda muy bien en la declaración conjunta emitida por la Presidencia del Comité del Convenio 108 y el Comisionado de Protección de Datos del Consejo de Europa el 30 de marzo de 2020[29]. En el contexto de la seguridad pública se han aplicado medidas de vigilancia y seguimiento y restricciones similares a las libertades básicas. Como consecuencia, se cuenta con un cúmulo de experiencia significativo a favor de la conciliación de la seguridad nacional con los derechos fundamentales, asegurando que las medidas que afectan la privacidad estén previstas en la ley y sean necesarias y proporcionadas en una sociedad democrática. Sin embargo, transferir esa experiencia al campo de la salud pública podría no ser tan sencillo, y podría ser necesario realizar ciertos ajustes para adoptar un enfoque apropiado que tenga en cuenta la privacidad y la protección de los datos.

65. Casi el 30 % de los Estados Miembros de las Naciones Unidas ya se han comprometido oficialmente, en virtud del derecho internacional, a respetar los

[26] El plazo para la presentación del presente informe solo permitió llevar a cabo un análisis esquemático de unos pocos países en los que se podía acceder más fácilmente a datos fiables. En el período comprendido entre junio de 2020 y junio de 2021, el Relator Especial se propone reunir y cotejar datos que permitan obtener un panorama más preciso y fiable de las medidas jurídicas y operacionales relacionadas con la COVID-19 disponibles y aplicadas en el Sur Global. La situación de la COVID-19 en Asia, África y América del Sur, por ejemplo, todavía es muy incipiente y está siendo constantemente vigilada por el titular del mandato, que tiene la intención de informar al respecto en su próximo informe anual.

[27] ACNUDH, “COVID-19: los Estados no deben abusar de las medidas de emergencia para reprimir los DD HH – Expertos de la ONU”, comunicado de prensa, 16 de marzo de 2020. Puede consultarse en www.ohchr.org/SP/NewsEvents/Pages/DisplayNews.aspx?NewsID=25722&LangID=S.

[28] Véanse también Tribunal Europeo de Derechos Humanos, *Lawless v. Ireland* (núm. 3), sentencia de 1 de julio de 1961, párr. 3; y *Denmark, Norway, Sweden and the Netherlands v. Greece* (solicitudes núms. 3321, 3322, 3323 y 3324/67), informe de la Comisión Europea de Derechos Humanos de 5 de noviembre de 1969.

[29] Consejo de Europa, “Joint Statement on the right to data protection in the context of the COVID-19 pandemic by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe”, Estrasburgo, 30 de marzo de 2020. Puede consultarse en https://rm.coe.int/covid19-joint-statement/16809e09f4.

principios de necesidad y proporcionalidad: los 55 Estados que han ratificado el Convenio 108 o el Convenio 108+ del Consejo de Europa ya están obligados por el artículo 9 del Convenio 108 o el artículo 11 del Convenio 108+. Deben tener muy presente que las medidas adoptadas en interés de la salud pública deben satisfacer las mismas pruebas de legalidad, necesidad y proporcionalidad en una sociedad democrática que están previstas en los artículos mencionados. A los efectos del presente informe, se entiende que la situación de la COVID-19 está comprendida en el artículo 11, párrafo 1, subpárrafo a del Convenio 108+, en la sección referida a "otros objetivos esenciales de interés público general". Por consiguiente, un primer paso para el 70 % restante de los Estados Miembros que no son partes en el Convenio sería aprovechar la recomendación anterior del Relator Especial y adherirse al Convenio 108+ lo antes posible, para luego poner en marcha todos los mecanismos señalados en el presente documento y en otros, y aplicar sus principios a la gestión cotidiana, incluida la protección de los datos relacionados con la salud.

66. Así pues, cuando un Estado tenga una ley que prevea facultades extraordinarias y cuando las medidas que se apliquen en el ejercicio de esas facultades parezcan invadir la vida privada, incluida cualquier forma de vigilancia (por ejemplo, geolocalización, vigilancia de proximidad, programas maliciosos, escuchas telefónicas o aplicación de perfiles), se deberán supervisar *ex ante* y *ex post* para demostrar que son necesarias y proporcionadas respecto del objetivo perseguido. De esa manera, se garantizaría que solo se utilice el método de vigilancia adecuado, con el propósito adecuado y durante el tiempo que sea conveniente, y que esté a cargo de las personas apropiadas.

## E. La tecnología y otras realidades

67. Entre los diversos medios tecnológicos a los que han recurrido los Gobiernos en respuesta a la pandemia de COVID-19, las aplicaciones de teléfonos inteligentes han sido uno de los métodos más estudiados o utilizados por los Estados para vigilar la propagación del virus. Hasta ahora, muchos países parecen haber tomado la decisión de desarrollar sus propias aplicaciones para el rastreo de contactos. Por lo tanto, la interoperabilidad transfronteriza sigue siendo apenas un deseo y una recomendación para el futuro[30].

68. Los siguientes son algunos de los aspectos que se han tenido en cuenta para desarrollar las aplicaciones de rastreo de contactos:

a) La forma en que la aplicación reúne información sobre la ubicación o la proximidad de las personas (por ejemplo, algunas aplicaciones identifican los contactos de una persona rastreando los movimientos del teléfono inteligente, utilizando el Sistema de Posicionamiento Global o la triangulación de torres de telefonía móvil cercanas) y busca otros teléfonos que hayan estado en la misma ubicación al mismo tiempo;

b) El uso del rastreo de proximidad, en el que los teléfonos inteligentes intercambian fichas cifradas con otros teléfonos cercanos a través de la señal de

[30] Cabe destacar que, si bien se ha hecho todo lo posible por garantizar la exactitud de la información brindada, la situación relativa a la COVID-19 ha limitado en gran medida la capacidad del Relator Especial para cotejar los datos, especialmente los obtenidos de los informes de medios de comunicación. Por lo tanto, la información que figura en el presente informe sobre las prácticas o respuestas actuales de diversos Estados se ofrece como posiblemente indicativa, y no necesariamente definitiva. Se espera que esta información, si la situación de la COVID-19 lo permite, se verifique adecuadamente y se refleje en un informe en 2021.

Bluetooth, y se maneja la información reunida y su almacenamiento (es decir, enfoques centralizados frente a descentralizados);

c) Si la instalación y el uso de la aplicación son de carácter voluntario u obligatorio (es decir, uso consensuado frente a no consensuado).

69. Muchas aplicaciones dependen de las interfaces de programación de aplicaciones conjuntas desarrolladas por Apple y Google. La interfaz permite que los teléfonos inteligentes iOS y Android se comuniquen entre sí a través de Bluetooth, lo que permitió a los desarrolladores diseñar una aplicación de rastreo de contactos que funciona para ambos. Las dos empresas tienen previsto incorporar esta capacidad directamente en sus sistemas operativos.

70. Uno de los problemas más graves, en general, es que no se da la debida importancia a la subdisciplina de la ingeniería de la privacidad. Las empresas de tecnología más grandes, como Apple, fueron de las primeras en introducir la ingeniería de la privacidad como enfoque disciplinario específico. Es importante subrayar que no basta con depender únicamente de las garantías jurídicas. La privacidad debe ser considerada desde el principio, comenzando con la ingeniería de la aplicación. Aunque esa idea está prevista en el espíritu del enfoque de "privacidad desde el diseño" propugnado en el Reglamento General de Protección de Datos de la Unión Europea, la realidad de la ingeniería de la privacidad no se acerca en absoluto a tan elevados ideales. En la práctica, la gran mayoría de los países del mundo cuentan con equipos de ingeniería de tecnología de la información y las comunicaciones para quienes el núcleo del proceso de ingeniería son el desempeño o la funcionalidad, y no la privacidad. La escasez de formación e investigación en materia de ingeniería de la privacidad en las universidades significa que se necesitarán varios años, posiblemente decenios, para que la situación cambie y la privacidad desde el diseño se convierta en una realidad.

71. Sin embargo, son motivo de cierta esperanza las acciones concertadas de pequeños grupos de personas motivadas. Una práctica prometedora desarrollada en respuesta a la situación generada por la COVID-19 es el Rastreo Descentralizado de Proximidad para Preservar la Privacidad, un protocolo abierto desarrollado por un grupo de facultades de ingeniería[31] para el rastreo basado en Bluetooth, en el que los registros de contacto del teléfono inteligente de una persona solo se almacenan localmente, por lo que ninguna autoridad central puede saber quién ha estado expuesto. Varios Estados (como Alemania, Austria, Estonia y Suiza) han anunciado que las aplicaciones que han desplegado a nivel nacional se basan en este protocolo. Por otro lado, el Rastreo Paneuropeo de Proximidad para Preservar la Privacidad, otro protocolo desarrollado en respuesta a la pandemia de COVID-19 por un consorcio de académicos y agentes comerciales, carece de ciertas características de transparencia y preservación de la privacidad (por ejemplo, los datos de los usuarios se almacenan en un servidor, mientras que el Rastreo Descentralizado de Proximidad para Preservar la Privacidad tiene una capacidad descentralizada, de modo que los datos nunca salen del teléfono inteligente del usuario).

72. Según el diseño de la aplicación, es posible que los funcionarios de salud no puedan acceder a los datos sobre las personas a las que se ha acercado una persona infectada. Algunas aplicaciones, como COVIDSafe (Australia) y StopCovid (Francia), tienen un diseño centralizado, lo que significa que la persona infectada debe cargar la identificación de su teléfono inteligente y la de los teléfonos de sus

[31] École Polytechnique Fédérale de Lausanne, ETH Zurich, KU Leuven, Universidad Tecnológica de Delft, University College de Londres, Centro Helmholtz para la Seguridad de la Información, Universidad de Turín y Fundación ISI.

contactos recientes en un servidor central. Aunque las identificaciones se anonimizan, los funcionarios pueden ver toda la red de contactos.

73. Otras aplicaciones, como la que se emplea en Alemania, están descentralizadas, de manera que los datos sobre los contactos recientes de una persona permanecen en su teléfono inteligente. Una persona infectada solo sube su propia identificación anonimizada a una base de datos central; cualquier persona que tenga la aplicación en su teléfono puede subir periódicamente la lista de usuarios infectados y comprobar si hay teléfonos a los que se haya acercado recientemente. Los defensores de la privacidad ven grandes ventajas en este diseño y sostienen que no implica ninguna vulnerabilidad de los datos sobre las redes sociales de los usuarios ante la piratería o la explotación.

74. La importancia de los datos de los teléfonos inteligentes para la investigación médica también es pertinente y debe tenerse en cuenta, ya que es una razón ampliamente invocada por los Estados que optan por el diseño centralizado. En el caso de las aplicaciones descentralizadas, los investigadores y los departamentos nacionales de salud pública solo tienen conocimiento de las personas que llaman para informar de que han recibido una notificación. Dado que los agentes de la salud pública no tienen acceso a los números telefónicos de las personas que han sido notificadas y que no han informado de una notificación, podría ser más difícil evaluar la exactitud y la precisión de los datos captados por la aplicación.

75. Hay una diferencia esencial entre la forma en que se promueven las aplicaciones o se obliga a su uso. La mayoría de los Estados alientan a los ciudadanos a descargar la aplicación de manera voluntaria, con el libre consentimiento del usuario. La India es el único país democrático que ha hecho que la descarga de la aplicación sea obligatoria para millones de personas. En algunos casos infrecuentes, pero importantes, el uso de la aplicación se ha declarado obligatorio para ciertas categorías de personas, por ejemplo, en la República de Corea, o incluso para cualquiera que disfrute de una vida normal, como en China.

76. Incluso cuando la instalación de la aplicación es “voluntaria”, la entrada obligatoria de datos varía y es importante evaluar el nivel de protección de los datos asegurándose de que la aplicación solo capte la información necesaria, que el almacenamiento de los datos respete las normas internacionales de protección de datos y que dicho almacenamiento esté limitado en el tiempo y se utilice solo con los fines adecuados.

### Sistemas híbridos de vigilancia

77. El método de vigilancia aplicado en la República de Corea incorporaba el uso de una aplicación para teléfonos inteligentes, pero no se basaba únicamente en ella, sino que empleaba un enfoque híbrido que reunía tecnologías utilizadas convencionalmente en la aplicación de la ley y la lucha contra el terrorismo, y combinaba varias fuentes de datos personales para obtener un panorama de los movimientos de una persona, entre otras cosas:

– Las transacciones con tarjetas de crédito y de débito, que pueden indicar dónde ha comprado o comido una persona, y su uso de una red de transporte;

– Los registros de ubicación de teléfonos obtenidos de los operadores de telefonía móvil, que dan una idea aproximada del vecindario en el que se encuentra una persona cuando se conecta a las diferentes antenas de telefonía;

– Detalles capturados por la extensa red de cámaras de vigilancia[32].

[32] Rory Cellan-Jones, “Tech Tent: Can we learn about coronavirus-tracing from South Korea?”, *BBC News*, 15 de mayo de 2020. Puede consultarse en www.bbc.com/news/technology-

78. El sistema empleado en Israel no solo está basado en las tecnologías de lucha contra el terrorismo, sino que las utiliza directamente. Se ha informado de que, desde mediados de marzo, la Agencia de Seguridad de Israel viene ayudando al Gobierno de Israel a realizar investigaciones epidemiológicas proporcionando al Ministerio de Salud los recorridos de los portadores del coronavirus y listas de personas con las que han estado en estrecho contacto[33]. Esa información está disponible en la base de datos de metadatos de comunicaciones de la Agencia. El método de vigilancia utilizado en Israel es particularmente interesante dado que el Tribunal Supremo de Israel invalidó su uso en abril de 2020, lo que obligó al Gobierno a aprobar una nueva ley para proporcionar el fundamento jurídico correcto para ese tipo de vigilancia. Aunque desde marzo el Gobierno de Israel ha tratado de fortalecer el nivel de control parlamentario de sus operaciones de inteligencia, a diferencia de los Países Bajos, el Reino Unido y otros países, no cuenta con un "órgano de expertos" independiente establecido por ley que pueda actuar como autoridad de supervisión completamente independiente para complementar la labor del Comité Parlamentario.

# III. Conclusiones

79. **Las actividades de vigilancia y de rastreo de contactos relacionadas con la COVID-19 pueden adoptar diversas formas y pueden ser manuales o tecnológicas, anónimas o no, y consensuadas o no.**

80. **A fin de evaluar adecuadamente las medidas adoptadas para hacer frente a la COVID-19, es importante determinar si son moderadamente útiles, si son indispensables, o si no son útiles en absoluto. Esa evaluación ayudaría a determinar si la medida es necesaria y proporcionada en una sociedad democrática y, por lo tanto, permisible en virtud del derecho internacional en materia de privacidad.**

81. **Es demasiado pronto para evaluar definitivamente si algunas medidas relacionadas con la COVID-19 podrían ser innecesarias o desproporcionadas. El Relator Especial seguirá observando los efectos de las actividades de vigilancia con fines epidemiológicos sobre el derecho a la privacidad[34] y presentará informes a la Asamblea General en 2021. El principal riesgo para la privacidad radica en el uso de métodos no consensuados, como los que se esbozan en la sección sobre sistemas híbridos de vigilancia, que podrían dar lugar a una desviación de la función y ser utilizados para otros fines que pueden afectar la privacidad.**

82. **La vigilancia tecnológica intensiva y omnipresente no es la panacea para situaciones de pandemia como la de COVID-19. Esto se ha puesto de manifiesto sobre todo en los países en los que el uso de métodos convencionales de rastreo de contactos, sin recurrir a aplicaciones de teléfonos inteligentes, geolocalización u otras tecnologías, ha resultado ser más eficaz para combatir la propagación de la COVID-19.**

83. **Si un Estado determina que es preciso aplicar medidas de vigilancia tecnológica como respuesta a la pandemia mundial de COVID-19, debe**

52681464.

[33] Amir Cahane, "Israel reauthorizes Shin Bet's coronavirus location tracking", *Lawfare*, 3 de julio de 2020. Puede consultarse en www.lawfareblog.com/israel-reauthorizes-shin-bets-coronavirus-location-tracking.

[34] El Relator Especial está compilando cuadros que contienen datos básicos sobre el uso de la tecnología en relación con la COVID-19, que se actualizarán para reflejar la información más exacta. Los cuadros se publicarán como apéndice del presente informe de 2020 a la Asamblea General en el sitio web del titular del mandato (www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx) y se actualizarán según sea necesario.

**asegurarse, tras demostrar tanto la necesidad como la proporcionalidad de las medidas específicas, de disponer de una ley que prevea tales medidas explícitamente (como en el ejemplo de Israel).**

84. **Un Estado que desee introducir una medida de vigilancia a los efectos de la COVID-19 no debería poder basarse en una disposición jurídica genérica, como la que establece que la jefatura de la autoridad de salud pública puede "ordenar que se tome cualquier otra medida que considere apropiada". Eso no proporciona salvaguardias explícitas y específicas, que son obligatorias tanto en virtud de las disposiciones del Convenio 108 y del Convenio 108+ como de la jurisprudencia del Tribunal Europeo de Derechos Humanos. De hecho, si una salvaguardia no se explica con suficiente detalle, no puede considerarse adecuada.**

85. **La OMS mantiene una lista de casos de COVID-19 (y muertes) por región de la OMS[35]. La lista sirve de recordatorio constante de que es necesario dar prioridad a la adopción de medidas que reduzcan significativamente las muertes. En pocas palabras, si un Estado desea utilizar una medida que afecta la privacidad, especialmente cuando sería fácil abusar de ella, como la vigilancia tecnológica, el Estado debe demostrar que la medida es necesaria y proporcionada para lograr el objetivo perseguido. El Estado en cuestión debe someter la medida a una prueba estricta formulando las siguientes preguntas: ¿Hubo o hay otro método que pueda utilizarse que hubiera evitado las muertes en la misma medida o mejor que la tecnología desplegada o contemplada que afecta la privacidad? ¿La tecnología desplegada fue o es una "salida fácil"? ¿Cuál es el costo de desplegar esa tecnología en particular, ya sea económico o en lo relativo a la privacidad? Solo entonces se podrá evaluar adecuadamente la necesidad y el costo de aplicar medidas que no afectan la privacidad, así como la proporcionalidad de esas medidas.**

86. **Es comprensible que algunos de los Estados que han adoptado tecnologías que afectan la privacidad para combatir la COVID-19 afirmen que han rastreado una cierta cantidad de casos o han evitado una cierta cantidad de muertes. Sin embargo, esas afirmaciones aún no han sido verificadas. Es demasiado pronto para evaluar adecuadamente la eficacia de las medidas adoptadas en relación con la COVID-19 y para dar respuesta a las siguientes preguntas:**

**a) ¿Qué funciona?**

**b) ¿Qué funciona mejor?**

**c) ¿Qué funciona mejor para quién?**

**d) ¿Qué funciona mejor en qué lugar?**

87. **Una vez individualizada una medida, la siguiente pregunta es: ¿por qué funcionó o funciona mejor esta medida, para quién y dónde? Se espera que las pruebas que se obtengan en los próximos 12 meses permitan comprender mejor estas variables y otras, lo que ayudaría a los expertos en materia de privacidad a evaluar adecuadamente las medidas adoptadas contra la COVID-19, y determinar si las medidas no consensuadas cumplen las estrictas pruebas de proporcionalidad y necesidad.**

---

[35] OMS, Coronavirus disease (COVID-19), Situation report. Puede consultarse en www.who.int/docs/default-source/coronaviruse/situation-reports/20200712-covid-19-sitrep-174.pdf?sfvrsn=5d1c1b2c_2. Cabe destacar que, en esta etapa, no está nada claro si la eficacia en la reducción de la mortalidad debe ser el único o el principal criterio para evaluar las medidas adoptadas contra la COVID-19. Se requieren más consultas para determinarlo.