Naciones Unidas A/76/220

Asamblea General

Distr. general
23 de julio de 2021
Español
Original: inglés

Septuagésimo sexto período de sesiones
Tema 75 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 sobre el derecho a la privacidad, Joseph A. Cannataci, presentado de conformidad con la resolución 28/16 del Consejo.

* A/76/150.

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, se propone contribuir a dilucidar cómo puede gestionarse una pandemia respetando el derecho a la privacidad. Se trata de un análisis algo más concluyente realizado a partir del informe que el Relator Especial presentó a la Asamblea General en 2020 (A/75/147), ahora que se dispone de más datos empíricos que permiten llevar a cabo una evaluación más precisa de la actual pandemia de enfermedad por coronavirus (COVID-19). El Relator Especial examina, en particular, las repercusiones de las medidas adoptadas contra la COVID-19 en la protección de datos, la tecnología y la vigilancia, y señala que las medidas en curso adoptadas por los Estados para combatir la propagación de la COVID-19 siguen afectando negativamente al disfrute del derecho a la privacidad y la personalidad y a otros derechos humanos conexos. El informe contiene recomendaciones dirigidas a los agentes estatales y no estatales para reforzar la privacidad y la personalidad; salvaguardar el acceso de los niños a la enseñanza en línea; proteger la privacidad de la información; y garantizar la transparencia y la medición.

I. Introducción

1. Si bien la pandemia de enfermedad por coronavirus (COVID-19) sigue evolucionando, ahora se dispone de una mayor cantidad de material que permite saber el modo en que la gestión actual de la pandemia puede integrar mejor el derecho a la privacidad al adoptar medidas eficaces de salud pública.

2. La cuestión que se planteaba en el informe presentado por el Relator Especial a la Asamblea General en 2020 (A/75/147) sobre si vulnerar el derecho a la privacidad en caso de pandemia es lícito, proporcionado y necesario, y en qué medida, tenía por objeto aclarar cuál es el enfoque más adecuado frente a pandemias presentes y futuras. La pregunta sigue sin respuesta. Existe una falta de datos precisos y comparativos; además, la mala preparación de los Estados ante la pandemia y las deficiencias en la rendición de cuentas, junto con sus respectivos contextos políticos, han contribuido a esta opacidad.

3. En todo caso, la finalidad del presente informe es contribuir a dilucidar cómo puede gestionarse una pandemia en relación con el derecho a la privacidad. El informe se basa en gran medida en la consulta pública sobre la COVID-19 convocada por el Relator Especial, junto con la Asamblea Global de Privacidad y la Organización de Cooperación y Desarrollo Económicos, celebrada del 21 al 23 de junio de 2021, y en otras investigaciones[1].

II. Privacidad y personalidad y enfermedad por coronavirus

4. Muchas de las medidas adoptadas por los Estados para contener la propagación de la COVID-19 han repercutido negativamente en el disfrute del derecho a la privacidad y otros derechos humanos. Los efectos negativos se han visto exacerbados por la desigualdad estructural existente, la exclusión social y las privaciones. Esta crisis de salud pública ha puesto de manifiesto la interdependencia entre los Estados y el sector empresarial, así como la interrelación entre el género, la raza, el origen étnico y la situación socioeconómica, y los resultados sanitarios. Las medidas para contener la propagación del virus han supuesto restricciones a los derechos humanos que, si bien afectan al conjunto de la ciudadanía, tienen un efecto desproporcionado en algunos sectores de la sociedad[2].

5. El Relator Especial ha promovido una interpretación más amplia de lo que es la privacidad que va más allá de la privacidad de la información[3] y la vigilancia, y ha destacado el aspecto positivo y facilitador del derecho a la privacidad en relación con la dignidad humana, la contribución de la privacidad al disfrute de otros derechos humanos y su importancia en el desarrollo de la personalidad del individuo. Ello es coherente con un enfoque según el cual la privacidad se considera no como un derecho humano en el vacío, sino más bien en el contexto de su relación con otros derechos, en especial con los que facilita o posibilita. Así pues, la privacidad es un requisito esencial para poder ejercer el derecho al libre desarrollo de la personalidad, reconocido explícitamente en el artículo 22 de la Declaración Universal de los Derechos Humanos de 1948: “Toda persona... tiene derecho a obtener... la satisfacción

[1] Merecen mención especial la profesora Elizabeth M. Coombs, el Sr. Ketan Modh y el Sr. Halefom Abraha por su colaboración en la elaboración y edición del presente informe.

[2] “Epidemics have gendered effects” Clare Wenham, profesora asociada de Política Santiaria Mundial, Escuela de Economía y Ciencias Políticas de Londres, cita de Martha Henriques, 13 de abril de 2020. Véase: www.bbc.com/future/article/20200409-why-covid-19-is-different-for-men-and-women.

[3] A veces se utiliza erróneamente de forma intercambiable con su subconjunto “privacidad de los datos”.

de los... derechos... indispensables a su dignidad y al libre desarrollo de su personalidad". El artículo 29 de la Declaración también protege el derecho a desarrollar la personalidad: "toda persona tiene deberes respecto a la comunidad, puesto que solo en ella puede desarrollar libre y plenamente su personalidad". Uno de los ejemplos más claros de la relación entre el derecho a la privacidad y el derecho a la personalidad en el discurso de las Naciones Unidas desde la publicación de la Declaración puede encontrarse en la resolución 34/7 del Consejo de Derechos Humanos sobre el derecho a la privacidad en la era digital, en la que el Consejo reconoce "que el derecho a la privacidad puede permitir el disfrute de otros derechos y el libre desarrollo de la personalidad y la identidad de las personas, y su capacidad para participar en la vida política, económica, social y cultural, y observan con preocupación que las violaciones o transgresiones del derecho a la privacidad podrían afectar al ejercicio de otros derechos humanos, como el derecho a la libertad de expresión y a abrigar opiniones sin injerencias, y el derecho a la libertad de reunión y asociación pacíficas". Por lo tanto, la evaluación exhaustiva de los derechos humanos con relación a la eficacia de las medidas anti-COVID debe tener en cuenta una serie de derechos que están estrechamente entrelazados en el marco de una complejidad cada vez mayor debido a una serie de tecnologías, en particular el acceso a Internet, la fotografía y la telefonía, que convergen principalmente en el uso de los teléfonos inteligentes.

6. Como se subraya claramente en el texto, el primer informe del Relator Especial sobre la pandemia de COVID-19[4] fue necesariamente, al igual que el presente documento, un informe provisional basado únicamente en los datos disponibles, realizado transcurridos tan solo cuatro meses desde el inicio de la pandemia. Por consiguiente, su principal objetivo era señalar cuáles eran las autoridades competentes y el fundamento jurídico de las medidas de salud pública y el derecho a la privacidad. Ese informe no contemplaba los efectos de las medidas antipandémicas en los diferentes aspectos de la vida privada ni el impacto diferencial de las medidas contra la COVID en los distintos grupos de la sociedad, en especial, en los que se encuentran en situación de vulnerabilidad y marginación. Esas importantes cuestiones reflejan la calidad de una sociedad y de sus instituciones de gobierno. La incorporación eficaz, o no, de todos los derechos humanos en la gestión de la pandemia es un indicador de esa calidad.

7. En su informe presentado al Consejo de Derechos Humanos en 2021 (A/HRC/46/37), el Relator Especial señaló el efecto de la COVID-19 en la privacidad de los niños. El cierre de escuelas afectó aproximadamente al 90 % de la población estudiantil mundial. En 2020, las descargas de aplicaciones educativas aumentaron en un 90% en comparación con la media semanal de finales de 2019.

8. El paso a la enseñanza en línea amplificó los desequilibrios de poder existentes entre las empresas de tecnología aplicada a la educación y los alumnos, y entre los Gobiernos y los alumnos y los padres. Varios Gobiernos dejaron en suspenso las leyes de privacidad sobre los datos de los niños. En otros lugares, por ejemplo, en algunos estados australianos, no existe ninguna protección del derecho a la privacidad de los niños en las escuelas públicas, pese a que agentes no estatales suelen controlar los expedientes escolares digitales de los niños. Esos registros digitales incluyen rasgos relativos al razonamiento, trayectorias de aprendizaje previstas, puntuaciones sobre el nivel de participación, tiempos de respuesta, páginas leídas y vídeos vistos.

[4] A/75/147.

9. No se puede separar la gestión de la pandemia de la educación; del mismo modo, tampoco se puede ignorar la relación entre la educación, la privacidad y la gestión de la pandemia. Cuando la pandemia obligue a que cada vez un mayor número de clases se imparta en línea, las consecuencias para la privacidad pueden quedar ocultas, aunque sean graves. Esto es absolutamente cierto, pues en la mayoría de los países la educación es obligatoria desde una edad temprana y la mayor parte de los niños y los padres no pueden impugnar los acuerdos de privacidad de las empresas de tecnología educativa o negarse a proporcionar datos a pesar de que sus preocupaciones son legítimas. Por ejemplo, a finales de 2020, se analizaron 496 aplicaciones de tecnología educativa en 22 países y se constató que muchas recopilaban los identificadores de los dispositivos; 27 aplicaciones recogían los datos de la ubicación y 79 de las 123 aplicaciones analizadas manualmente facilitaban los datos de los usuarios a terceros, como a socios publicitarios. Se han indicado los riesgos de seguridad de los datos. Por ejemplo, Microsoft informó de 5,7 millones de incidentes con programas maliciosos que afectaron a los usuarios de sus programas educativos entre el 24 de agosto y el 24 de septiembre de 2020[5].

10. La adopción de medidas aparentemente sencillas para contener el coronavirus ha tenido consecuencias imprevistas; algunas de esas medidas son importantes para la protección de la privacidad de la persona. La designación de días diferentes en que los hombres y las mujeres pueden salir de sus casas para realizar actividades esenciales, como adquirir alimentos o acudir a los servicios de salud[6], ha afectado negativamente a las comunidades transgénero[7]. Restringir la libre circulación de las personas en función de su género aumenta el riesgo de que las personas lesbianas, gais, bisexuales, transgénero e intersexuales (LGBTQI) sean “descubiertas” y maltratadas en los controles de identidad de las fuerzas de seguridad y la policía. Desde que se declaró la pandemia, en muchos Estados también se ha considerado “no esencial” la atención médica de afirmación de género, que a menudo salva vidas.

11. La integridad física y la autonomía están vinculadas a la privacidad. Por su propia naturaleza, los entornos domésticos son espacios más privados, pero el confinamiento en un entorno doméstico durante una pandemia puede ser problemático por otras razones. Durante los confinamientos, se registró un aumento de la violencia de género infligida en el hogar por la pareja u otros miembros de la familia[8]. En el caso de algunos niños, las medidas de confinamiento han aumentado el riesgo de ser objeto de violencia física o psicológica en el hogar y han limitado la posibilidad de ponerse en contacto con adultos a quienes pudieran informar de esos actos violentos[9].

12. Las evaluaciones de los derechos humanos antes y durante la pandemia deberían haber mitigado los riesgos indicados anteriormente y, por lo tanto, son un componente esencial de la orientación en materia de políticas de cara al futuro.

---

[5] Véase Quentin Palfrey and others, “Privacy considerations as schools and parents expand utilization of Ed Tech apps during the COVID-19 pandemic”, International Digital Accountability Council, 1 de septiembre de 2020. Disponible en: https://digitalwatchdog.org/wp-content/uploads/2020/09/IDAC-Ed-Tech-Report-912020.pdf.

[6] Por ejemplo, Panamá y el Perú, entre otros. Véase: www.reuters.com/article/us-health-cronavirus-peru-idUSKBN21K39N, abril de 2020.

[7] La identidad de género forma parte de la privacidad. Véase Comité de Derechos Humanos, *G. v. Australia*, (CCPR/C/119/D/2172/2012), párr. 7.2.

[8] Véase COVID-19 y el aumento de la violencia de género y la discriminación contra la mujer, llamamiento conjunto de la Plataforma EDVAW de mecanismos de expertos independientes sobre la discriminación y la violencia contra la mujer, relativo a la lucha contra la pandemia de violencia de género contra la mujer durante la crisis de COVID-19, 20 de julio de 2020. Disponible en https://rm.coe.int/edvaw-statement-covid-19-and-vaw-final/16809efd2c.

[9] A/HRC/46/19, párr. 17.

III. Privacidad, otros derechos humanos y la enfermedad por coronavirus

13. La pandemia ha planteado cuestiones sobre los derechos y su lugar en una democracia. En 10 de los 13 países encuestados, tanto en 2020 como en 2021 el sentimiento de división social ha aumentado considerablemente desde que se inició la pandemia[10]. Por ejemplo, si bien los pasaportes de vacunación pretenden mejorar el ejercicio de los derechos y suavizar las restricciones de viaje, estos excluyen a quienes no tienen acceso a vacunación, no pueden vacunarse por motivos de salud o deciden no hacerlo. El porcentaje de la población mundial que pertenece en conjunto a esas categorías es actualmente muy elevado[11].

14. Personas de todo el mundo han cedido aspectos de su privacidad y sus libertades en favor de sus Gobiernos para contener la propagación del coronavirus. Las medidas adoptadas por los países han afectado a la libertad de expresión (57 países); a la libertad de reunión (147 países); y al derecho a la privacidad (60 países)[12]. Es preciso evaluar la proporcionalidad y la necesidad de esas intervenciones.

15. Mientras las medidas de vigilancia de la COVID-19 se mantengan e incluso se amplíen, los Gobiernos tendrán un mayor acceso a los datos personales relativos a la ubicación, el historial médico y cualquier otra información confidencial sobre la vida y las finanzas de la población. Es muy probable que algunos Estados no renuncien a sus nuevas prerrogativas e instrumentos de vigilancia masiva una vez que la crisis sanitaria haya remitido. En China, una aplicación creada para el seguimiento del coronavirus se está implantando de forma permanente en algunas ciudades. Y lo que es más preocupante: hay un nuevo sistema que utiliza programas informáticos para decretar cuarentenas y permite enviar datos personales a la policía, lo que constituye un alarmante precedente de control social automatizado[13]. Supuestamente, esos riesgos son más pronunciados en Asia[14], pero en todos los países, incluso en las democracias, las autoridades pueden explotar los datos con fines políticos, con la consiguiente merma de derechos humanos. Las medidas de emergencia antipandémicas entrañan riesgos que requieren medidas de protección de calidad para situaciones de emergencia[15].

IV. Protección de datos, tecnología, vigilancia y enfermedad por coronavirus

16. Los datos relacionados con la COVID-19 son datos sanitarios, que constituyen la primera categoría de datos personales que pueden ser objeto de niveles especiales de protección en virtud de la legislación internacional, regional y nacional. En octubre de 2019, el Relator Especial presentó a la Asamblea General un marco integral para

[10] Véase la encuesta de Pew Research Center del 1 de febrero al 26 de mayo de 2021, entre 18.850 adultos de 17 economías avanzadas. Disponible en: www.pewresearch.org/fact-tank/2021/06/24/eu-seen-favorably-across-17-advanced-economies-but-views-vary-on-its-coronavirus-response/.

[11] Véase OECD, “Access to COVID-19 vaccines: global approaches in a global crisis”, OECD Policy Responses to Coronavirus (COVID-19) (18 de marzo de 2021).

[12] Véase International Center for Not-for-Profit Law, COVID-19 Civic Freedom Tracker. Disponible en: www.icnl.org/covid19tracker/?issue=5.

[13] Paul Mozur, Raymond Zhong y Aaron Krolik, *In Coronavirus fight, China gives citizens a color code, with red flags*, The New York Times, 1 de marzo de 2020, actualizado el 28 de enero de 2021.

[14] Véase Sofia Nazalya, “Human Rights Outlook 2020”, 30 de septiembre de 2020.

[15] Véase Graham Greenleaf, “COVID-19: the available evidence…and a little bit of hindsight”. 23 de junio de 2021).

la protección de los datos sanitarios, que fue objeto de una serie de recomendaciones exhaustivas[16] y de un detallado memorando explicativo[17]; sin embargo, se calcula que aproximadamente el 75% de los Estados Miembros de las Naciones Unidas dista mucho de cumplir las normas establecidas en esos documentos. Todos los datos disponibles indican que esas deficiencias se han agravado con la pandemia de COVID-19.

17. Para dar respuestas efectivas a las crisis sanitarias es necesario reunir y gestionar datos confidenciales, lo que requiere rigurosas medidas de protección de la privacidad. Sin embargo, en muchos casos no se establecieron ni se han establecido sistemas que limiten el procesamiento de datos a lo estrictamente necesario para fines específicos relacionados con la salud.

18. En numerosos países no existen garantías de transparencia en relación con el procesamiento de datos ni salvaguardias contra las filtraciones de datos. En otros, no se han respetado los requisitos de protección de datos en vigor; por ejemplo, el Certificado Digital COVID de la Unión Europea propuesto por la Comisión Europea el 17 de marzo de 2021, un año después de que se declarara la pandemia en marzo de 2020, no se ha sometido a una evaluación de impacto: dada la urgencia, la Comisión no realizó una evaluación de impacto[18].

19. Esas deficiencias socavan los esfuerzos de los organismos de salud pública y la confianza de los ciudadanos en ellos. Por ejemplo, el 60 % de los estadounidenses cree que si el Gobierno rastreara la ubicación de las personas por medio de sus teléfonos móviles no supondría una gran diferencia en lo que respecta a la contención de la COVID-19[19].

20. Los datos son un elemento fundamental en muchas de las medidas adoptadas contra la pandemia, por lo que con el paso del tiempo la COVID-19 también se ha convertido en una “crisis de datos”. En la actualidad, los Gobiernos y las empresas tecnológicas procesan datos personales y datos sobre la salud de la población. Ello suscita dudas acerca de la necesidad y la proporcionalidad de los datos recogidos, los métodos de recopilación, la seguridad y los usos secundarios de esos datos[20]. Un motivo de especial preocupación para las personas LGBTQI es que se divulguen datos sanitarios sin el consentimiento del interesado[21]. Casi la mitad de los australianos (48 %) están hoy más preocupados por la protección de sus datos de localización debido a la COVID-19, mientras que tres cuartas partes (75 %) opinan que la COVID-19 no exime ni a las empresas ni a las administraciones públicas de cumplir con sus obligaciones ordinarias con arreglo a lo dispuesto en las leyes sobre protección de la privacidad[22].

[16] www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/UNSRPhealthrelateddataRecCLEAN.Pdf.

[17] www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/MediTASFINALExplanatoryMemoradum1.pdf.

[18] Véase Memorándum explicativo de la propuesta de la Comisión de la Unión Europea, secc. 3. Disponible en: eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0130.

[19] Véase la encuesta Pew Research Center realizada en abril de 2020. Disponible en: www.pewresearch.org/fact-tank/2020/05/04/how-americans-see-digital-privacy-issues-amid-the-covid-19-outbreak/.

[20] *Ibid*.

[21] A/HRC/40/63 2019, párr. 84.

[22] Oficina del Comisionado de la Información de Australia, 2020.

Tecnología

21. La tecnología utilizada para gestionar la pandemia se divide en cuatro grandes grupos:

a) instrumentos de rastreo de contactos y distanciamiento físico basados en el seguimiento de proximidad por bluetooth;

b) códigos de respuesta rápida (códigos QR) o códigos de barras utilizados para registrarse en locales;

c) acceso a los datos de geolocalización mediante el uso del historial de las torres de telefonía móvil o el Sistema de Posicionamiento Global (GPS) para localizar los lugares en los que sea preciso alertar a la población por su posible proximidad a personas que hayan tenido un resultado positivo en las pruebas de COVID-19;

d) aplicaciones para pedir cita para vacunarse o para descargar un certificado de vacunación.

22. Algunas tecnologías carecen de datos que demuestren su precisión. Hay indicios que apuntan a que las tecnologías en uso no son fiables. Por ejemplo, en Israel, muchas personas han impugnado con éxito las medidas de cuarentena a que habían sido sometidas mediante el uso de la triangulación de torres de telefonía móvil. De las 20.000 personas que presentaron un recurso contra su orden de aislamiento, el 54% (aproximadamente 12.000) consiguieron su objetivo[23]. En los Estados Unidos de América, American Civil Liberties Union informó de que los datos de las torres de telefonía eran imprecisos[24].

23. También se ha comprobado que el seguimiento de proximidad por Bluetooth carece de fiabilidad. En un estudio realizado sobre la implantación del seguimiento de proximidad por Bluetooth en tranvías europeos en Alemania, Italia, y Suiza, se comprobó que la fiabilidad de la detección era similar a la emisión de notificaciones por selección aleatoria[25]. La fiabilidad depende de la intensidad de la señal, que se ve afectada por: las diferencias entre los distintos modelos y marcas de teléfonos; las fluctuaciones en la orientación relativa de los teléfonos; la absorción por el cuerpo humano o las fundas; y la reflexión de las ondas de radio en las paredes, el suelo y los muebles.

Vigilancia de pandemias mediante el uso de datos

24. “Vigilancia” es un término técnico que se utiliza en los estudios epidemiológicos y la contención de enfermedades. También se utiliza para referirse a las labores de seguridad relacionadas con la recopilación de información y la aplicación de la ley, entre otras cosas. Ambos usos, el médico y el relativo a la seguridad, deben ser necesarios y proporcionados.

[23] “Over 12,000 mistakenly quarantined by phone tracking, Health Ministry admits”, *The Times of Israel*, 14 de julio de 2020.

[24] Véase Jay Stanley and Jennifer Stisa Granick, “The limits of location tracking in an epidemic” (8 de abril de 2020).

[25] Véase Douglas J. Leith and Stephen Farrell, “Measurement-Based Evaluation of Google/Apple Exposure Notification application programme interface for Proximity Detection in a Light-Rail Tram” (2020) PLOS One, vol. 15, e0239943.

25. La necesidad de proteger la salud de la población obligó a los países a adoptar medidas de vigilancia para hacer un seguimiento de la propagación de la infección mediante:

a) el rastreo manual de contactos, como en Malta[26];

b) el uso de Bluetooth y GPS, el rastreo mediante torres de telefonía móvil, el uso de códigos de barras o códigos QR en los móviles y la utilización de tecnología ponible en sistemas específicamente diseñados para su uso en epidemias, como, por ejemplo, en la República de Corea;

c) el uso de torres de telefonía móvil y otras fuentes de triangulación de datos originalmente concebidas como medidas antiterroristas encubiertas, pero reconvertidas para su uso en situaciones de pandemia, como, por ejemplo, en Israel;

d) el registro obligatorio mediante códigos de barras y códigos QR[27], como en Australia;

e) el uso de pasaportes de vacunación, por ejemplo, el Reglamento sobre el Certificado COVID Digital de la Unión Europea, que entró en vigor el 1 de julio de 2021[28].

26. La recogida y el tratamiento de los datos procedentes de esas fuentes difieren mucho en todo el planeta, en cuanto al tipo de datos recopilados, el lugar donde se almacenan, quién tiene acceso a ellos y la autonomía de las personas cuyos datos se recogen. Muchos de los datos son producto de las respuestas tecnológicas, así como también una aportación a ellas. La estructura tecnológica es importante en lo que atañe a las opciones de que disponen los ciudadanos para gestionar determinados aspectos de su derecho a la privacidad.

27. Las aplicaciones de rastreo de contactos pueden seguir un enfoque centralizado o descentralizado con respecto a los datos para el rastreo de contactos o para el registro de vacunas. Los enfoques centralizado y descentralizado se distinguen principalmente por el lugar donde se almacenan los datos y por cómo se procesan. Según el enfoque centralizado, los datos de los usuarios se almacenan y procesan en un servidor central gestionado por las autoridades de salud pública o en el servidor de una empresa privada elegida por el Gobierno, con independencia de dónde se generen.

28. En el caso de las aplicaciones de rastreo de contactos, los servidores calculan las puntuaciones de riesgo actualizadas de todos los usuarios pertinentes y deciden con qué usuarios afectados deben ponerse en contacto. En el registro de vacunas, los servidores almacenan los datos sobre los períodos de vacunación programados, el tipo de vacunación y el estado de cada persona con fines administrativos.

29. En lo que respecta a las autoridades, los sistemas centralizados permiten analizar los datos recogidos para conocer cómo se propaga la pandemia, las zonas más afectadas y la cobertura de vacunación, entre otras cosas. Ello facilita la asignación de recursos con arreglo a las prioridades establecidas.

[26] Jessica Arena, “What is contact tracing and how is Malta doing it?” *Times of Malta*, 23 de marzo de 2020.

[27] Véase, por ejemplo, Gobierno de Australia Meridional, “COVID SAfe Check-In” (disponible en: www.covid-19.sa.gov.au/business-and-events/covid-safe-check-in) y Gobierno de Nueva Gales del Sur, “Setting up electronic check-in and QR codes” (disponible en: www.nsw.gov.au/covid-19/covid-safe/customer-record-keeping/setting-up-electronic-check-and-qr-codes).

[28] Véase https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_es.

30. Australia dispone de dos sistemas centralizados: una aplicación de proximidad por Bluetooth (COVIDSafe) y un programa de seguimiento por código QR para el registro de eventos. La aplicación COVIDSafe se implantó mediante la promulgación de una ley específica que preveía medidas para salvaguardar la privacidad. Sin embargo, el programa de rastreo mediante códigos QR no está respaldado por ninguna ley especial, sino que depende de los reglamentos sanitarios anteriores y de la Ley de Privacidad vigente de 1988. Esta carencia es problemática, pues Australia no cuenta con garantías constitucionales sobre el derecho a la privacidad.

31. La República de Corea estableció un sistema centralizado basado en el uso de registros de establecimientos de salud, datos obtenidos por GPS, transacciones con tarjetas y circuitos cerrados de televisión[29], teniendo en cuenta la experiencia adquirida anteriormente por el país con el brote del síndrome respiratorio de Oriente Medio (MERS) en 2015. El enfoque permitió determinar las rutas utilizadas por los pacientes, el riesgo de exposición para otras personas de su entorno, la clasificación de los contactos en estrechos y ocasionales y la gestión de esos contactos mediante medidas de cuarentena.

32. La Argentina también puso en marcha una base de datos centralizada para la recopilación de datos a partir de la aplicación Cuidar, que se creó mediante una decisión administrativa el 23 de marzo de 2020[30]. Si bien es voluntario para los residentes en la Argentina, era obligatorio para los viajeros procedentes del extranjero; el Gobierno nacional y los gobiernos provinciales pueden acceder a los datos obtenidos por medio de Bluetooth.

33. La arquitectura centralizada, como la de Australia, Israel y la República de Corea, suscita preocupación en cuanto a la protección y el almacenamiento seguro de información confidencial, en particular, los datos sanitarios, así como respecto de la elevada probabilidad de que los Gobiernos y las empresas utilicen las bases de datos centralizadas para otros fines, como la vigilancia política y comercial.

34. Los ciudadanos desconfían de la creación por los Gobiernos de bases de datos a gran escala con su información. Por ejemplo, la mayoría de los australianos (60 %) acepta que se hagan algunas concesiones con relación a la protección de la privacidad para combatir la COVID-19 por el bien común, siempre que sean temporales. Sin embargo, más de la mitad (54 %) manifiesta una mayor preocupación por la protección de su información personal debido a la gestión de la COVID-19, entre los que figura un 26 % que se muestra muy preocupado[31].

35. Las aplicaciones descentralizadas proporcionan a los usuarios un mayor control sobre su información. Esta se almacena en sus teléfonos, en lugar de en una base de datos central a la que pueden acceder el Gobierno u otras entidades. Entre los ejemplos de un enfoque descentralizado ampliamente adoptado se encuentra la interfaz de programación de aplicaciones del sistema de notificación de exposición de Google y Apple (Google-Apple Exposure Notification System), mediante la que los avisos no se procesan por medio de una base de datos central, sino que se activan de forma automática, en el propio teléfono de los usuarios.

36. Algunos países han optado por un conjunto de medidas centralizadas y descentralizadas. Singapur distribuyó dispositivos de rastreo ponibles por Bluetooth

[29] Véase “Contact transmission of COVID-19 in South Korea: novel investigation techniques for tracing contacts” *Osong Public Health and Research Perspectives*, vol. 11, núm. 1 (2020), pags. 60 a 63.

[30] Disponible es: www.boletinoficial.gob.ar/detalleAviso/primera/227116/20200324.

[31] Véase 2020 Australian Community Attitudes to Privacy Survey. Disponibe en: www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page/2020-australian-community-attitudes-to-privacy-survey/.

para que registraran todas las interacciones con otros dispositivos de rastreo situados en las inmediaciones, y conservó esos datos durante 25 días antes de eliminarlos[32]. Ese enfoque ha permitido crear aplicaciones para teléfonos móviles para el rastreo de contactos, aplicar medidas de cuarentena, hacer un seguimiento de los síntomas y proporcionar información sobre la pandemia; en agosto de 2020 ya se habían detectado 46 aplicaciones[33].

37. Entre las consideraciones relativas a la arquitectura técnica se encuentra la cuestión de si las tecnologías adoptadas son obligatorias o voluntarias. Una aplicación puede considerarse voluntaria si el usuario tiene la posibilidad de rechazarla:

a) no instalando la aplicación;

b) desactivando la función Bluetooth/GPS;

c) utilizando la aplicación, pero negándose a informar de un diagnóstico positivo.

38. Si bien la respuesta inicial a las aplicaciones de rastreo voluntario de contactos en Israel y Australia fue positiva, lo cierto es que solo un pequeño porcentaje de la población las utilizó. En Australia, la Ley sobre la modificación de la privacidad (Información de contacto para la salud pública) de 2020 ("Ley COVIDSafe") tipificó como delito la obligatoriedad del uso de la aplicación COVIDSafe[34]. La valoración inicial de la población fue positiva, ya que el 70% de los encuestados la apoyó, aunque ahora la aplicación está "prácticamente abandonada"[35]. Los Gobiernos de los distintos Estados australianos parecen confiar más en la obligatoriedad de registrarse en los locales mediante códigos QR. La República de Corea llevó a cabo una iniciativa de ámbito nacional que aplicó el rastreo obligatorio de la ubicación desde su puesta en marcha, y hay quienes atribuyen los buenos resultados en la contención de la pandemia al carácter obligatorio de esa política[36].

39. La capacidad de otorgar consentimiento y de retirarlo forma parte del derecho a la privacidad. Es imposible ejercer esa facultad si las aplicaciones de rastreo de contactos son obligatorias. Las medidas obligatorias también conllevan el riesgo de que los Gobiernos y las empresas hagan un uso indebido de los datos recogidos para combatir la pandemia mediante la "infiltración de la vigilancia" o la reutilización de los datos sin que los proveedores de datos tengan la posibilidad de eliminarlos de las bases de datos.

---

[32] Véase "TraceTogether, safer together". Disponibe en: www.tracetogether.gov.sg/.

[33] Véase Hanson John Leon Singh, Danielle Couch and Kevin Yap, "Mobile health apps that help with COVID-19 management: scoping review", *JMIR Nursing*, vol. 3, núm. 1 (2020), e20596.

[34] Véase la sección 94H la Ley sobre la modificación de la privacidad (Información de contacto para la salud pública) de 2020 (*Privacy Amendment (Public Health Contact Information) Act 2020*):

1) Cometerá un delito toda persona que exija a otra persona que:
   a) descargue la aplicación COVIDSafe en un dispositivo de comunicación; o
   b) tenga COVIDSafe en funcionamiento en un dispositivo de comunicación; o
   c) dé su consentimiento para transferir los datos de la aplicación COVID desde un dispositivo de comunicación al Depósito Nacional de Datos COVIDSafe.

Pena: cinco años de prisión o 300 unidades de multa, o ambas cosas.

[35] Paul M. Garrett and Simon J. Dennis, "Australia has all but abandoned the COVIDSafe app in favour of QR codes (so make sure you check in)", *The Conversation*, 1 de junio de 2021.

[36] Véase Kyung Sin Park, "Korea's COVID-19 success and mandatory phone tracking" (opennet, 20 de octubre de 2020).

Traspasar los límites

40. Muchos países estaban mal preparados para gestionar el aumento de infecciones y muertes. Algunos consideraron que era imperativo hacer frente a los riesgos para la salud y la vida de sus ciudadanos por todos los medios disponibles. Ya sea a sabiendas o sin saberlo, las medidas adoptadas por algunos Gobiernos han supuesto una transgresión en lo que respecta al derecho de los derechos humanos y a lo que es adecuado y apropiado en una sociedad democrática.

41. En ocasiones, los medios disponibles para llevar a cabo operaciones de vigilancia por "razones de salud pública" y por motivos de inteligencia o seguridad se han fusionado y desdibujado, y se ha perdido una importante delimitación y diferenciación. En contextos en los que se han adoptado medidas voluntarias con el apoyo de la ciudadanía, tales conductas por parte de los Estados ponen de manifiesto que el derecho a la privacidad y a la autonomía de los ciudadanos se está soslayando.

Israel

42. A fin de ilustrar el problema derivado del intento de obviar los derechos, cabe señalar que el Gobierno de Israel declaró el estado de emergencia el 19 de marzo de 2020 por medio de la Ordenanza de Salud Pública de 1940[37]. El Ministerio de Salud empleó una aplicación, "HaMagen", que recopilaba la información de los movimientos y la ubicación de los usuarios y la almacenaba en la memoria interna de sus dispositivos móviles, a menos que los usuarios optaran por enviar esos datos al Ministerio de Salud, donde los empleados, los representantes y los proveedores de servicios podían acceder a ellos. Así pues, la aplicación tenía un uso descentralizado, a la vez que centralizado (de forma voluntaria).

43. Junto con ese arreglo, el Gobierno de Israel autorizó a la Agencia de Seguridad del país a que solicitara y recopilara datos de las torres de telefonía de los proveedores de servicios de telecomunicaciones sin el consentimiento de las personas sometidas a vigilancia. Los proveedores de servicios de telecomunicaciones se vieron obligados a rastrear los movimientos de las personas que se sabía que estaban infectadas a partir de los registros de las torres de telefonía móvil, en virtud de dos decretos consecutivos sobre emergencias de mediados de marzo de 2020, en los que se autorizaba a la policía a pedir esos datos para localizar a los pacientes, llevar a cabo comprobaciones aleatorias de las personas sometidas a cuarentena y rastrear sus movimientos durante un máximo de 14 días[38]. En abril de 2020, el Tribunal Supremo de Israel invalidó el método de vigilancia utilizado, lo que obligó al Gobierno a aprobar una nueva ley que proporcionara un fundamento jurídico adecuado para autorizar a la Agencia a seguir realizando los rastreos conforme a la ley de la Agencia de Seguridad de Israel. A ello le siguió, en julio de 2020, la ley temporal de autorización de la Agencia de Seguridad de Israel.

44. A principios de 2021, mediante la modificación temporal de la Ordenanza de Salud Pública de 1940 se autorizó la transferencia de información personal de personas no vacunadas a los municipios y a los funcionarios de educación y asistencia social. A principios de marzo de 2021, el Tribunal Supremo del país prohibió que se recurriera a la ley relativa a la autorización para la vigilancia masiva y, a continuación, suspendió la aplicación de la modificación.

[37] Greenleaf, "COVID-19: the available evidence … and a little bit of hindsight" (véase la nota a pie 15).

[38] Véase David M. Halbfinger, Isabel Kershner and Ronen Bergman, "To track Coronavirus, Israel moves to tap secret trove of cellphone data", *The New York Times*, 16 de marzo de 2020.

45. Además, se ha informado de que los datos de vacunación se han utilizado para: la investigación de grandes grupos de población sin su consentimiento; la divulgación pública de las vías de infección; el uso de drones para la vigilancia de la cuarentena domiciliaria; el uso por empresas de datos genéticos para las pruebas de COVID-19 y la difusión de un proyecto de ley para la transferencia de información epidemiológica a la policía[39].

46. Al principio, la aplicación descentralizada HaMagen, que puso en marcha el Ministerio de Salud, fue valorada positivamente y permitió detectar el 30% de los casos iniciales, pero su uso se redujo drásticamente debido a la pérdida de confianza de la población en las garantías de privacidad de la aplicación[40]. El rastreo de contactos de la Agencia parece haber tenido una eficacia reducida a causa de:

a) La falta de datos claros sobre los beneficios del programa de la Agencia, en términos absolutos y comparativos;

b) La tendencia de la tecnología a proporcionar falsos positivos.

47. El sistema utilizado en Israel usa tecnologías antiterroristas y está inspirado en ellas. Según se ha informado, desde mediados de marzo de 2020, la Agencia de Seguridad de Israel viene ayudando al Gobierno del país 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. La información procede de la base de metadatos de comunicaciones de la Agencia. Desde marzo, el Gobierno de Israel ha tratado de fortalecer el nivel de control parlamentario de sus operaciones de inteligencia. A diferencia de Francia, los Países Bajos y el Reino Unido de Gran Bretaña e Irlanda del Norte, Israel no cuenta con un "órgano de expertos" independiente establecido por ley que actúe como autoridad de supervisión independiente y complemente la labor de la comisión parlamentaria, por lo que las dudas acerca de la capacidad de llevar a cabo un control minucioso y eficaz de esas actividades por un servicio de inteligencia siguen siendo considerables. Aproximadamente un año después de la implantación de tecnologías que vulneran la privacidad para su uso en caso de pandemia, la trasgresión por Israel de los límites establecidos fue condenada de manera definitiva el 1 de marzo de 2021 por el Tribunal Supremo, quien prohibió al Gobierno el uso generalizado de sistemas de rastreo de los portadores del coronavirus mediante teléfonos móviles y calificó la medida de grave vulneración de las libertades civiles[41]. El Relator Especial señala algunos informes que indican que, en el caso de Israel, esas actuaciones también han frenado el desarrollo de aplicaciones que respeten la privacidad y permitan realizar investigaciones epidemiológicas, y considera que el uso de facultades antiterroristas en un entorno puramente sanitario es contrario al derecho internacional de los derechos humanos y sienta un peligroso precedente.

República de Corea

48. Otros Gobiernos, como el de la República de Corea, también obligaron a los proveedores de servicios de telecomunicaciones a rastrear los movimientos de quienes

[39] Prof. Yuval Shany, Israel's response to the COVID-19 pandemic: Right to Privacy Aspects, Federmann Cyber Security Research Centre, Hebrew University of Jerusalem; "COVID-19: the available evidence … and a little bit of hindsight" (véase la nota a pie 15).

[40] Véase, por ejemplo, Mitnick J, "How Israel's COVID contact tracing app rollout went wildly astray" (CIO, 7 de noviembre de 2020).

[41] Véase Maayan Lubell, *Israeli Supreme Court bans unlimited COVID-19 mobile phone tracking*. Disponible en: www.reuters.com/article/us-health-coronavirus-israel-surveillanc-idUSKCN2AT279.

se sabía que estaban infectados[42]. Las medidas de vigilancia aplicadas incorporaban el uso de una aplicación para teléfonos inteligentes que reunía tecnologías utilizadas convencionalmente en la aplicación de la ley y en la lucha contra el terrorismo, y combinaba varias fuentes de datos personales que ayudaban a formarse una idea de los movimientos de una persona, entre ellas:

a) las transacciones con tarjetas de crédito y de débito, que pueden indicar dónde ha comprado o comido una persona, y el uso que ha hecho de una red de transporte;

b) los registros de ubicación de teléfonos obtenidos a partir de los operadores de telefonía móvil, que ofrecen una idea aproximada del barrio en el que se encuentra una persona al conectarse a las diferentes antenas de telefonía;

c) detalles captados por la extensa red de cámaras de vigilancia.

49. En primer lugar, cabe señalar que, en la mayoría de los casos indicados, las medidas que invadían la privacidad relacionadas con la pandemia de COVID-19 adoptadas en la República de Corea tenían un fundamento jurídico: estaban previstas en la ley. Por consiguiente, las cuestiones pendientes siguen siendo las de siempre: ¿eran o son esas medidas necesarias y proporcionadas en una sociedad democrática?

50. Para responder a esa pregunta con precisión, es importante examinar en detalle lo que realmente ocurrió en la República de Corea. No cabe duda de que las tecnologías empleadas permitieron reducir drásticamente el tiempo necesario para detectar el foco de la infección y su propagación.

51. Cuando la COVID-19 empezó a propagarse, el Gobierno de la República de Corea transformó la plataforma de datos “Smart City” que estaba desarrollando en un instrumento de rastreo de salud pública. La Agencia de Control y Prevención de Enfermedades de Corea creó un sistema de apoyo a la investigación de epidemias, una plataforma que permite a las autoridades de salud pública recopilar y analizar datos con rapidez para rastrear los casos confirmados de COVID-19. El sistema empezó a funcionar el 26 de marzo de 2020, apenas dos meses después de que se confirmara el primer caso de COVID-19 en el país. Mediante este sistema, una vez que la Agencia confirma un caso de COVID-19, una serie de investigadores autorizados solicitan los datos de localización de cada paciente, y las entidades correspondientes los introducen en el sistema con arreglo a la Ley de Control y Prevención de Enfermedades Infecciosas del país. A continuación, el sistema analiza el rastreo en tiempo real, lo que se complementa con entrevistas convencionales realizadas por rastreadores de contactos humanos. Ello permite rastrear con celeridad los contactos y localizar los focos más activos de infección de la pandemia. El sistema ha permitido rastrear e investigar casos confirmados de COVID-19 en menos de 10 minutos, en lugar de en un día o más, como ocurría antes. La confidencialidad y la seguridad de los datos se garantizan cerciorándose de que únicamente puedan acceder al sistema los investigadores de la Agencia con la autoridad legal pertinente y registrando cada ingreso al sistema para detectar posibles incidentes de seguridad. Para reducir al mínimo los datos personales recopilados, el periodo máximo de recogida de datos para cada caso está fijado en 14 días, que es el periodo de incubación de la enfermedad. Además, el sistema tiene un carácter temporal: al final de la pandemia de COVID-19, toda la información personal será destruida[43].

[42] Véase Kyung Sin Park, “Korea’s COVID-19 success and mandatory phone tracking” (véase la nota a pie 36).

[43] Véase Jiyeon Kim and Neil Richards “South Korea’s COVID success stems from an earlier infectious disease failure”, 29 January 2021. Dispobible en: https://slate.com/technology/2021/01/south-korea-mers-covid-united-states-democracy.html.

52. El Sistema de Apoyo a la Investigación Epidemiológica descrito anteriormente es la primera de varias medidas de índole tecnológica adoptadas por el Gobierno. En segundo lugar, la República de Corea ha utilizado una aplicación para teléfonos inteligentes que permite supervisar el cumplimiento de la normativa vigente por las personas sometidas a aislamiento o cuarentena, es decir, los casos confirmados de COVID-19, las personas que están en estrecho contacto con un caso confirmado y los viajeros internacionales. A lo largo de la pandemia, la República de Corea no ha cerrado sus fronteras a ningún viajero internacional que desee entrar en el país. En su lugar, ha aplicado procedimientos especiales de entrada que obligan a mantener una cuarentena de 14 días y a realizar pruebas gratuitas de diagnóstico de la COVID-19 para evitar la propagación de la enfermedad. La aplicación Self-Quarantine Safety Protection es una aplicación bidireccional que permite a la persona en cuarentena informar de cualquier síntoma y al funcionario designado para el caso supervisar el cumplimiento de la cuarentena mediante los datos de ubicación obtenidos por GPS previo consentimiento. Si bien se recomienda encarecidamente hacer un seguimiento del cumplimiento de la cuarentena mediante la aplicación, ello no es obligatorio. Las personas que no dispongan de teléfonos inteligentes o que no deseen utilizar la aplicación pueden someterse a vigilancia mediante el método tradicional de llamadas telefónicas por el funcionario encargado del caso. No obstante, a 1 de septiembre la tasa de adopción de la aplicación era del 91,8 % y tanto los ciudadanos de la República de Corea como los viajeros están tranquilos al saber que quienes corren el riesgo de propagar la enfermedad cumplen las medidas de cuarentena[44].

53. En el resumen que figura a continuación se explican algunas de las razones por las que el Relator Especial considera que la recopilación de una cantidad importante de datos personales en nombre de la lucha contra la pandemia de COVID-19 no fue, en determinados períodos de tiempo, especialmente durante el período comprendido entre enero y junio de 2020, ni necesaria ni proporcionada:

> La divulgación de los datos de rastreo de los contactos (por ejemplo, “dónde, cuándo y durante cuánto tiempo”) ayuda a identificar de forma autónoma a las personas con las que se ha estado en estrecho contacto cuya infección está confirmada. Sin embargo, divulgar el rastro de la ubicación puede conllevar riesgos en lo que respecta a la privacidad, pues permite deducir los lugares relevantes y los hábitos cotidianos de una persona. Los riesgos para la privacidad dependen en gran medida de los patrones de movilidad de una persona, que se ven afectados por varios factores regionales y normativos (como el tipo de residencia, los servicios cercanos y las órdenes de distanciamiento social). Además, los resultados indicaron que los datos del rastreo de contactos divulgados en la República de Corea a menudo incluyen información irrelevante, como datos demográficos precisos (por ejemplo, edad, sexo, nacionalidad), datos relativos a las relaciones sociales (por ejemplo, la casa de los padres) e información sobre el lugar de trabajo (por ejemplo, el nombre de la empresa). Divulgar esos datos de personas ya identificadas puede carecer de utilidad para el rastreo de contactos, cuyo objetivo es localizar a personas no identificadas que podrían mantener un contacto estrecho con personas que sean casos confirmados. Dicho de otro modo, para rastrear los contactos no tiene mayor utilidad divulgar el perfil personal del caso confirmado ni cuáles son sus relaciones sociales, como familiares y amigos. La ubicación precisa del lugar de trabajo podría omitirse ya que, en la mayoría de los casos, es fácil llegar a los empleados por medio de las redes de comunicación interna; un caso excepcional sería cuando existe la sospecha de una posible infección grupal con contagios

[44] *Ibid*.

secundarios. Tampoco es necesario desvelar información detallada de los viajes de las personas procedentes del extranjero (que no se haya comunicado en los resultados principales), como el número de vuelo de llegada y el objeto o la duración de los viajes internacionales[45].

54. Si bien el Relator Especial condena la mencionada recopilación de datos personales que, a primera vista, es innecesaria y desproporcionada, también señala los continuos y constantes intentos del Gobierno y las instituciones de la República de Corea por aumentar la protección de la privacidad a pesar de las medidas adoptadas contra la COVID-19, por ejemplo:

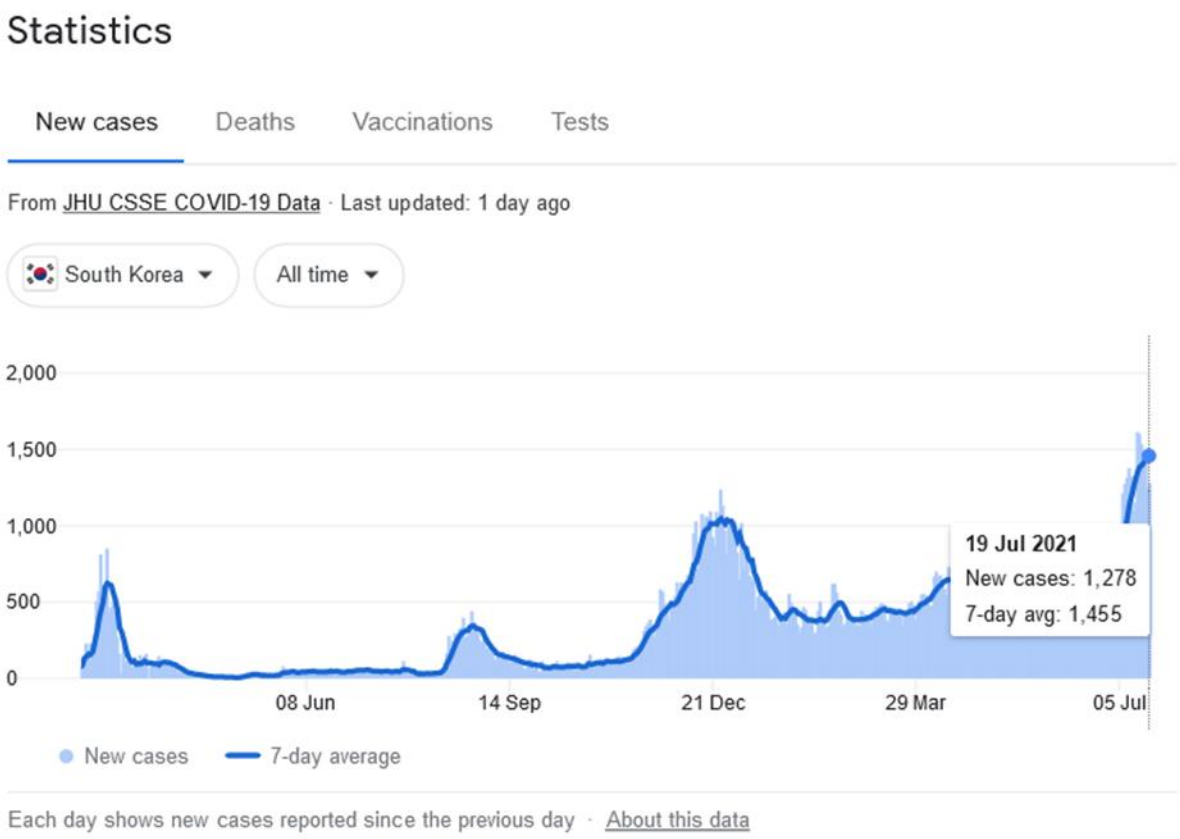
a) En junio y octubre de 2020, los Centros para el Control y la Prevención de Enfermedades emitieron una serie de orientaciones a fin de que no se publicaran la edad, el sexo, la nacionalidad, el lugar de trabajo, el historial de viajes o el lugar de residencia de los pacientes, si bien algunos gobiernos locales han seguido divulgando historiales de viajes individuales, pese a que se les ha indicado que no lo hagan. Continúa habiendo dudas en cuanto a la recogida y el tratamiento de información personal confidencial, que puede contener datos de carácter privado, como la orientación sexual y las relaciones personales de la persona.

b) En marzo de 2021, el Gobierno de la República de Corea pidió a la población que utilizara sus números personales encriptados, en lugar del número de teléfono, para proteger su privacidad cuando tuvieran que anotar los registros de entrada en restaurantes, cafeterías y demás, como parte de las medidas necesarias para prevenir la propagación de la COVID-19. En febrero de 2021, el Gobierno implantó una nueva medida de protección de la privacidad que permite a los ciudadanos utilizar números privados encriptados para visitar esos lugares. Un número encriptado consiste en una combinación de cuatro cifras y dos letras, y no puede utilizarse para realizar llamadas telefónicas o enviar mensajes de texto. Las autoridades únicamente pueden convertirlo cuando haya una necesidad urgente de contactar con el titular del número por motivos relacionados con un virus.

55. El Relator Especial concluye que, en su empeño por combatir la COVID-19, el Gobierno de la República de Corea adoptó una serie de medidas que vulneraban el derecho a la privacidad, que, en algunos casos, no eran ni necesarias ni proporcionadas. No obstante, en la mayoría de esos casos, si no en todos, el Gobierno entendió que se había equivocado y trató de subsanar sus errores mediante medidas correctivas (véanse los ejemplos anteriores).

56. En el gráfico se ilustra la evolución de las tres olas de COVID-19 sufridas durante la pandemia en la República de Corea entre marzo de 2020 y el 19 de julio de 2021.

[45] Véase Gyuwon Jung and others, “Too much information: assessing privacy risks of contact trace data disclosure on people with COVID-19 in South Korea”, *Frontiers in Public Health*, 18 de junio de 2020. Disponible en: www.ncbi.nlm.nih.gov/pmc/articles/PMC7314957/ y www.frontiersin.org/articles/10.3389/fpubh.2020.00305/full.



Fuente: Universidad Johns Hopkins.

57. El gráfico muestra que, si bien el nivel de infección descendió considerablemente tras la tercera ola en enero de 2021, en marzo y abril de 2021, se encontraba al mismo nivel que el máximo alcanzado en la primera ola en marzo de 2020, es decir, aproximadamente 530 nuevos casos al día. Sin embargo, el 19 de julio de 2021 había alcanzado su nivel más alto, con unos 1.300 nuevos casos de infección al día. En el momento de presentar este informe (20 de julio de 2021) no estaban claras las razones precisas de ese nivel de infección, pese a todas las medidas de protección de la privacidad adoptadas. Las conclusiones en esta fase únicamente pueden ser preliminares, dado que se necesita un mayor número de datos obtenido a lo largo de un período de tiempo más largo para poder llegar a conclusiones definitivas. Por lo tanto, aún está pendiente el veredicto final sobre si alguna o todas las medidas que afectan a la privacidad adoptadas por la República de Corea en relación con la pandemia de COVID-19 eran necesarias y proporcionadas. Ello dificulta la posibilidad de determinar la existencia de buenas prácticas, de haberlas, en el proceder del Gobierno con respecto a la privacidad en el contexto de la pandemia, salvo en el caso de las medidas correctivas relacionadas con la reducción de los datos personales que deben recogerse, adoptadas a lo largo de 2020 y 2021.

58. En Nigeria, las medidas de confinamiento aplicadas en todo el país se tradujeron en actos de represión mortíferos y en violaciones de los derechos humanos, si bien los casos de vulneración del derecho a la privacidad fueron probablemente de los menos graves en comparación con otros actos de consecuencias nefastas. Aparte de las restricciones a la libertad de circulación, se informó de que las fuerzas de

seguridad nigerianas habían practicado arrestos y detenciones ilegales, habían extorsionado y habían incautado y confiscado bienes[46].

59. Singapur también traspasó los límites innecesariamente. Su caso ilustra de forma notable el problema de la "deriva funcional". "El apoyo de la población se vio mermado después de que las autoridades revelaran en enero de 2021 que la policía había utilizado los datos de la aplicación en la investigación de un asesinato, apenas unos meses después de que el ministro responsable prometiera que únicamente se utilizarían para contener la COVID-19. Excepcionalmente, el Gobierno emitió una disculpa. Pero en lugar de echarse atrás, tiene previsto formalizar las competencias de la policía para que puedan acceder a esos datos en casos concretos, mediante la introducción de una ley que presentará al parlamento"[47]. En virtud de las modificaciones introducidas en la *Ley sobre la COVID-19 (Medidas Temporales) de 2020,* aprobadas por el Parlamento de Singapur en febrero de 2021, los datos personales recogidos por los programas digitales de rastreo de contactos de la pandemia solo podrán utilizarse para el rastreo de contactos, salvo que los requieran organismos encargados de hacer cumplir la ley para la investigación de "delitos graves"[48].

¿Quién está al mando aquí?

60. En abril de 2020, Google y Apple anunciaron un proyecto conjunto para posibilitar el uso de la tecnología Bluetooth con el fin de ayudar a los Gobiernos y a los organismos de salud a frenar la propagación del virus. La solución utilizaba interfaces de programación entre aplicaciones y tecnología basada en el sistema operativo para aumentar la privacidad y la seguridad de los usuarios mediante un modelo descentralizado[49]. La iniciativa de Google y Apple "Exposure Notification" marcó el rumbo de los enfoques descentralizados para el rastreo tecnológico de contactos mediante el móvil, debido a su dominio del mercado de los teléfonos inteligentes. Se ha utilizado en países de todo el mundo, como Australia, varios estados de Estados Unidos y la mayoría de los Estados miembros de la Unión Europea. En junio de 2020, el Gobierno del Reino Unido se vio obligado a dar un importante giro de 180 grados y abandonar el modo de funcionamiento de la aplicación de rastreo de coronavirus que tenía entonces, para pasar a un modelo basado en la tecnología proporcionada por Apple y Google.

61. En abril de 2021, una actualización de la aplicación de rastreo de contactos utilizada en Inglaterra y Gales quedó bloqueada por incumplir las condiciones de un acuerdo suscrito con Apple y Google[50]. El acuerdo que todas las autoridades de salud habían firmado para utilizar la tecnología de rastreo de contactos de Apple y Google, centrada en la privacidad, establecía la prohibición de recopilar datos de localización por medio del programa informático. Sin embargo, en la actualización propuesta, se pedía a los usuarios que subieran los registros de entrada a establecimientos (escaneos de códigos de barras de carteles) si daban positivo en la prueba del virus.

---

[46] Véase Simisola Akintoye, "*Privacy implications of national responses to COVID 19 in Nigeria"*; De Montfort University; Greenleaf, "COVID-19: the available evidence … and a little bit of hindsight" (véase la nota a pie 15); "Coronavirus: security forces kill more Nigerians than COVID-19", BBC News, abril de 2020.

[47] Véase Jamie Tarabay and Bloomberg, "Countries vowed to restrict use of COVID-19 data. For one Government, the temptation was too great", Fortune, 1 de febrero de 2021.

[48] Véase Kirsten Han, "*COVID app triggers overdue debate on privacy in Singapore"*, Al-Jazeera, 10 de febrero de 2021.

[49] Véase www.apple.com/mt/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/.

[50] Véase "Apple and Google block NHS Covid app update over privacy breaches", *The Guardian*, 20 de abril de 2021).

62. Esos incidentes ponen de manifiesto el poder de las grandes empresas tecnológicas. Con independencia de los aspectos jurídicos pertinentes y de la cuestión sobre qué organismo tenía la postura más favorable a la protección de la privacidad, es necesario someter a debate la conveniencia de que los Gobiernos deban recurrir al sector de la privacidad para suministrar instrumentos de salud pública a sus ciudadanos y sobre el poder de ese sector para dictar las condiciones en las que se proporcionarán esos instrumentos. Sin embargo, Francia ha demostrado que puede actuar en gran medida por su cuenta, dado que, en mayo de 2021, más del 25 % de la población francesa había descargado la aplicación puso en marcha en junio de 2020[51].

V. Atajos y otros mecanismos pandémicos

63. Muchos países no estaban suficientemente preparados para introducir en un corto espacio de tiempo medidas de salud pública como el distanciamiento físico, las restricciones a los viajes y el uso de mascarillas. Se tomaron atajos de diferentes formas y con diferentes consecuencias.

64. Los mecanismos han consistido, en primer lugar, en una declaración de estado de emergencia. Hasta la fecha, 108 países han emitido declaraciones de estado de emergencia[52], entre otras cosas, a fin de posibilitar la adopción de iniciativas de rastreo de contactos obligatorio. Por ejemplo, Sudáfrica emitió su declaración de estado de emergencia en virtud de la Ley de Gestión de Desastres de 2002.

65. En segundo lugar, se han establecido normas para eludir la protección de datos y la seguridad. En Austria, en marzo de 2020 se introdujeron modificaciones en la Ley de Sanidad Telemática de 2012 para permitir a los profesionales de la salud transferir datos sanitarios y genéticos mediante medios poco seguros, como el fax o el correo electrónico[53].

66. En tercer lugar, se han promulgado nuevas leyes. En marzo de 2020, Dinamarca aprobó la Ley sobre Epidemias, que limitaba:

a) el derecho de reunión, estableciendo toques de queda, restringiendo el acceso a determinadas zonas y prohibiendo reuniones y concentraciones (a partir de diez personas entre el 18 de marzo y el 8 de junio de 2020);

b) el derecho a la libertad personal, imponiendo la hospitalización, el aislamiento y la vacunación, y procediendo a la detención de personas sin infección confirmada;

c) el derecho al respeto de la privacidad mediante la implantación de aplicaciones de rastreo de contactos que incluyan requisitos que obliguen a las personas, las empresas y las autoridades públicas a proporcionar datos relacionados con la COVID-19, así como mediante soluciones basadas en datos que permitan examinar los movimientos, en particular de las personas.

67. En febrero de 2021 se modificó la Ley sobre Epidemias con el fin de introducir procedimientos parlamentarios y mecanismos de control relativos a: la adopción de normas y medidas intrusivas; el aumento de la transparencia y la reducción del poder arbitrario del Gobierno; la reducción de la implantación de medidas obligatorias

[51] Véase Reuters, “French COVID tracing app downloaded by 25 per cent of the population – minister”, 23 de mayo de 2021.

[52] A fecha 14 de julio de 2021, International Center for Not-for-Profit Law, “COVID-19 Civic Freedom Tracker” (véase la nota a pie 12).

[53] Véase la enmienda: www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20008120.

contra la persona permitiendo, por ejemplo, que la vacunación sea voluntaria; y el control judicial de las medidas obligatorias que conlleven penas privativas de libertad.

68. En cuarto lugar, en otros países, los organismos encargados de hacer cumplir la ley y las entidades civiles se convirtieron en agentes encargados de aplicar la normativa de salud pública. En abril de 2021, en virtud de la Ley de Salud Pública de Malta, el Director General de Salud Pública delegó su autoridad para hacer cumplir las medidas contra la pandemia en:

a) la policía y los funcionarios del organismo encargado del sistema local de aplicación de la ley;

b) las Fuerzas Armadas de Malta;

c) el Departamento de Transporte de Malta;

d) la Autoridad de Turismo de Malta;

e) la Dirección de Salud Ambiental.

69. Los funcionarios de los organismos mencionados estaban autorizados a entrar en un domicilio particular y llevar a cabo inspecciones a partir de una denuncia o de una sospecha razonable de que en su interior había una cantidad de personas reunidas que infringía la normativa. Esas medidas carecían de las garantías adecuadas y ponían en tela de juicio los principios de necesidad y proporcionalidad. Normalmente, la entrada en la vivienda de un particular requiere una orden judicial. Ese ejemplo pone de relieve el considerable alcance de las facultades relacionadas con las emergencias sanitarias.

70. La necesidad de definir las funciones y competencias de las autoridades de salud pública y de los organismos encargados de hacer cumplir la ley también se ha puesto de manifiesto en los llamamientos realizados por los organismos encargados de hacer cumplir la ley de otros países, como el Reino Unido, para que se permita la entrada en el domicilio de los presuntos infractores de las medidas de confinamiento por tratarse de un "instrumento útil" para hacer cumplir esas medidas[54].

VI. Otras consideraciones

71. La pandemia de COVID-19 sigue avanzando y el debate irá evolucionando a la par que ella. Actualmente, parte de ese debate se centra en el enfoque basado en los derechos humanos respecto de la privacidad adoptado por la Unión Europea, por ejemplo, frente al planteamiento a favor de la protección del consumidor adoptado por los Estados Unidos y, en cierta medida, por Australia. Recientemente, la Comisión Federal de Comercio de los Estados Unidos ha subrayado que es imperativo respetar la privacidad en el ámbito de la videoconferencia, la tecnología educativa y la tecnología sanitaria, y ha difundido cartas de advertencia y alertas de estafa en relación con la usurpación de identidad como consecuencia de haber pasado al teletrabajo y la escolarización digital[55].

72. Las crisis de salud pública anteriores han influido en la forma en que los países han afrontado la pandemia actual. Por ejemplo, la República de Corea utilizó mecanismos obligatorios y centralizados de rastreo de contactos debido al brote de MERS que sufrió en 2015. La experiencia anterior provocó la revisión de la Ley de

[54] Véase "Police Chief calls for power of entry into homes of suspected lockdown breakers", Vikram Dodd, *The Guardian*, 5 de enero de 2021.

[55] Véase Comisión Federal de Comercio, "One year into COVID-19 pandemic, new Federal Trade Commission staff report highlights agency's ongoing efforts to protect consumers", 19 de abril de 2021.

Control y Prevención de Enfermedades Infecciosas para proteger la confidencialidad de variables como el sexo, la edad, el nivel educativo y la nacionalidad, si bien se exigió que se informara obligatoriamente sobre el estado de la infección.

73. Las dimensiones geográficas de los países han afectado a la protección de la privacidad de ciertas medidas. Los países más pequeños han tenido cierta ventaja en el manejo de determinados aspectos de la pandemia: por ejemplo, a pesar de su alta densidad de población, Singapur pudo distribuir llaves digitales entre sus ciudadanos, lo que permitió poder utilizar la aplicación para teléfonos inteligentes TraceTogether a quienes no podían utilizar ese tipo de aplicaciones[56]. Por otro lado, países como la India, con una gran masa de territorio y de población, adoptaron el registro en línea y el registro mediante teléfonos inteligentes para la vacunación por medio de la aplicación CoWIN (conectada al número de teléfono individual), lo que no daba cabida a una gran parte de la población sin acceso a un teléfono inteligente o a Internet. Si bien proporcionar llaves digitales (o medios de registro alternativos o anónimos) requiere la emisión de muchos millones de esos dispositivos, no hacerlo es discriminatorio.

74. Aunque no son los únicos, África, América Latina, Australia y la India han sido señalados como regiones y países en los que no existen garantías constitucionales o leyes nacionales sólidas de protección de datos ni mecanismos de supervisión, y donde esa ausencia ha socavado los esfuerzos de los Gobiernos para garantizar la necesaria confianza de la ciudadanía en las medidas de salud pública.

75. En algunas partes del mundo, la existencia de leyes rigurosas de protección de datos de ámbito nacional y de organismos sólidos e independientes de protección de datos o de otros órganos de supervisión, facilita la puesta en marcha de iniciativas de rastreo de contactos y de registros de vacunación, teniendo debidamente en cuenta la necesidad de proteger los datos de los ciudadanos y de comunicar esa necesidad a la comunidad.

76. La mayoría de las medidas permiten recoger una gran cantidad de datos confidenciales y es difícil estimar si esa recopilación es proporcionada. Incluso leyes de protección de datos que se consideran sólidas, como el Reglamento General de Protección de Datos de la Unión Europea, requieren una mayor concreción y orientación para las situaciones de salud pública.

77. Los nuevos sistemas vienen a sumarse a la ya compleja infraestructura informática existente. Las autoridades de protección de datos de muchos países no pudieron llevar a cabo una evaluación de los aspectos técnicos de esos sistemas, ni de las largas descripciones sumamente técnicas que los acompañan, debido a los plazos o a la falta de recursos o de conocimientos técnicos, como señaló el Consejo de Protección de Datos de Austria (Datenschutzrat) en su evaluación de la iniciativa regional[57].

78. Por lo general, las estrategias utilizadas por los países de todo el mundo provocaron de forma inevitable la suspensión de los derechos humanos y las libertades fundamentales. Las medidas de emergencia facilitaron una respuesta rápida, pero no necesariamente bien concebida. Las aplicaciones para teléfonos inteligentes u otros medios de vigilancia deben ser jurídicamente aceptables, técnicamente fiables y socialmente asumibles, y deben someterse a una evaluación desde la óptica de los derechos humanos, que en gran medida brilló por su ausencia durante el periodo examinado.

[56] “Token Go Where”. Véase https://token.gowhere.gov.sg/.

[57] Véase www.bmj.gv.at/dam/jcr:c4b7569c-46c3-4772-bb07-9085f61412a8/Stellungnahme_des_Datenschutzrates_Epidemiegesetz.pdf.

79. La confianza de la población afecta a la eficacia de las medidas antipandémicas. Si bien es cierto que la confianza en el Gobierno desempeña un papel importante en el éxito de cualquier iniciativa gubernamental, esta es más necesaria en situaciones extraordinarias como en el caso de la pandemia de COVID-19. Ello es especialmente importante cuando se trata de medidas voluntarias cuya eficacia depende del compromiso de los ciudadanos.

80. Las medidas que invaden la privacidad han encontrado resistencia. En los Estados Unidos, el uso de medios de rastreo de la ubicación y los sistemas centralizados han encontrado una firme oposición; en julio de 2021, solo dos estados habían introducido pasaportes de vacunación, mientras que muchos estados los han prohibido[58]. A los ciudadanos les preocupa que las medidas contra la pandemia no se anulen. De forma similar, la mayoría de los australianos (60 %) está de acuerdo en que deben hacerse algunas concesiones a la protección de la privacidad para combatir la COVID-19 en aras del bien común, siempre que no sean permanentes[59].

81. La tecnología es un elemento fundamental para la gestión de los Gobiernos de los problemas de salud pública. Sin embargo, su uso podría normalizarse en las labores de vigilancia futuras después de la pandemia. Por ejemplo, las aplicaciones de rastreo de contactos impuestas por los Gobiernos también podrían utilizarse para acceder a los datos personales de los usuarios como medio de vigilancia gubernamental. La normalización del uso de tecnologías intrusivas allana el camino a otras medidas que invaden la privacidad. Así, las empresas han intensificado la vigilancia de sus trabajadores, y han introducido aplicaciones de seguimiento de la distancia física y llaves digitales.

82. La reticencia o la incapacidad de los Gobiernos para establecer el carácter proporcional y necesario de las medidas puede obedecer a la deriva funcional de las tecnologías y los datos recogidos, o a la ineficacia de esos instrumentos.

83. La pandemia ha dado lugar a problemas inesperados debido a que ha habido una evolución hacia entornos de trabajo híbridos, en los que la empresa vigila a los trabajadores de forma colectiva. Las medidas aplicadas por las empresas para monitorizar el distanciamiento físico entre los trabajadores han afectado a su privacidad. Mientras que muchas empresas han tenido que suspender sus actividades, otras han soslayado esa suspensión obligando a los trabajadores a que lleven puestos dispositivos de alerta de proximidad física. En la actualidad, muchas empresas desean vigilar a los empleados que teletrabajan mediante programas informáticos que registran las veces que se pulsan las teclas, las capturas de pantalla y otras tareas informáticas. Esas tecnologías podrían dar lugar a una “infiltración de la vigilancia”, mientras que el uso de otras deja patente que se está produciendo una “desviación del cometido”, ya que no almacenan localmente los datos registrados en los dispositivos de control ponibles, sino que los transmiten a una base de datos central sin que haya ninguna razón que lo justifique.

84. La pandemia de COVID-19 ha puesto de manifiesto las limitaciones de las leyes de protección de datos existentes para hacer frente a esos nuevos riesgos que afectan a los datos personales y a la privacidad. El Reglamento General de Protección de Datos, que por otra parte se considera que está marcando la pauta en materia de protección de datos en todo el mundo, no prevé la posibilidad de presentar

[58] Véase Elliott Davis, “Which States Have Banned Vaccine Passports?”, *US News*, 1 de junio de 2021.

[59] Oficina del Comisionado de la Información de Australia.

reclamaciones colectivas, dado que se ocupa principalmente de los derechos individuales[60].

VII. Conclusiones

85. Es en situaciones de emergencia cuando se constata la verdadera capacidad de los Estados, el Gobierno y los agentes privados, e incluso de los individuos.

86. Los tratados internacionales y la mayoría de las constituciones nacionales permiten a los Estados aumentar temporalmente sus facultades en períodos de crisis, como en el caso de la respuesta a la pandemia de COVID-19. La pandemia tiene consecuencias sanitarias, en materia de vigilancia y a nivel individual que están interrelacionadas. Por lo tanto, requiere que se gestione dentro de los parámetros establecidos para esos ámbitos.

87. Desde la perspectiva del derecho a la privacidad, la pandemia ha permitido una mayor intromisión de los Gobiernos y las empresas en la vida de las personas, vulnerando su derecho a la privacidad. Si bien es de esperar que durante una pandemia se produzcan algunas intromisiones por motivos de salud pública, hasta la fecha ha resultado imposible calibrar hasta qué punto estas han sido necesarias y proporcionadas.

88. Desafortunadamente, muchos Estados han considerado que la protección de la privacidad se opone a las medidas necesarias para salvar vidas. Se trata de una visión simplista que desconoce la importancia que la población concede a su privacidad y a limitar las intrusiones injustificadas del Gobierno y el sector privado en su vida. El resultado es la resistencia a las medidas adoptadas por el Gobierno para hacer frente a la pandemia.

89. La pandemia de COVID-19 ha propiciado que se tomen atajos en todo el mundo al aplicar las estrategias nacionales de salud pública. Algunos Gobiernos han hecho uso de leyes de emergencia para aprobar iniciativas obligatorias de rastreo de contactos; otros han aprovechado la falta de leyes rigurosas de protección de datos de ámbito nacional para poner rápidamente en marcha soluciones como el rastreo de contactos y el registro de personas vacunadas sin tener en cuenta el derecho a la privacidad y a otros derechos humanos. Entre las respuestas a la crisis, algunas de ellas precipitadas, figuran el recurso a las leyes de emergencia y a leyes de protección de datos deficientes o no existentes. La proximidad de las elecciones parece haber sido, y sigue siendo, un factor importante para algunos Estados y Gobiernos[61].

90. Los Estados Miembros se han servido de medios tecnológicos para rastrear los casos de infección, aplicar medidas de cuarentena, mantener normas de distanciamiento físico y hacer un seguimiento de la administración de vacunas. Esos instrumentos han sido creados por organismos gubernamentales y entidades empresariales.

91. En ese contexto, los países estaban mal preparados frente al ejercicio de la independencia y el poder de las empresas tecnológicas, como ilustra la postura adoptada por Apple y Google respecto de la privacidad de los usuarios de aplicaciones de rastreo de contactos. Al mismo tiempo, es importante reconocer que esas dos empresas parecen haber protegido la privacidad de forma razonable en su enfoque, en

[60] Véase Andrew Pakes, “High Visibility and COVID-19: returning to the post-lockdown workplace” (Ada Lovelace Institute, 19 de mayo de 2020).

[61] Véase www.idea.int/news-media/multimedia-reports/global-overview-covid-19-impact-elections.

ocasiones posiblemente con más rigor que algunos Estados que estaban dispuestos a utilizar los datos recopilados.

92. La pandemia actual exige que la promoción y la protección del derecho a la privacidad y de los derechos conexos sean objeto de un seguimiento continuo y de informes públicos por parte de organismos de ámbito internacional, regional y nacional.

93. Los enfoques centralizados, entre ellos los adoptados por Israel, Australia y la República de Corea, presentan riesgos para la privacidad, como los relativos a la protección y el almacenamiento de información confidencial, incluidos los datos sanitarios, la elevada probabilidad de que los Gobiernos y las empresas reutilicen esas bases de datos centralizadas y el riesgo de que se conserve un alto porcentaje de datos. Las aplicaciones descentralizadas proporcionan a los usuarios un mayor control sobre su información, dado que toda la información de contacto se guarda únicamente en el teléfono de los usuarios, y no hay una base de datos central a la que puedan acceder el Gobierno o las autoridades.

94. Las consecuencias para la privacidad del uso de aplicaciones de rastreo de contactos obligatorio son obvias: en muchos casos, aunque no en todos, la ley reconoce que el consentimiento y la posibilidad de retirarlo es un elemento fundamental del derecho a la privacidad. Las medidas obligatorias también aumentan el riesgo de que los Gobiernos y las empresas hagan un uso indebido de los datos confidenciales recopilados con el fin de combatir la pandemia, ya sea mediante prácticas que lleven a la "infiltración de la vigilancia" o la reutilización de los datos sin que los usuarios tengan la posibilidad de eliminar su información de las bases de datos. Las aplicaciones de rastreo de contactos voluntario han tenido una baja aceptación, normalmente debido a la falta de confianza de la población en la capacidad del Gobierno para garantizar la seguridad y protección de sus datos.

95. La tecnología también plantea muchos problemas a la hora de implantarla, como la falta de datos que permitan comprobar la precisión de algunas tecnologías. La mayoría de las medidas analizadas recogen muchos datos confidenciales y es difícil estimar si esa recopilación es proporcionada. Si bien la tecnología desempeña un papel fundamental en la pandemia, también puede hacer que la vigilancia se normalice en el futuro. La vigilancia tecnológica intensiva y omnipresente no es la panacea para situaciones de pandemia como la de COVID-19.

96. Otras cuestiones conexas son la igualdad y la protección de la privacidad de los trabajadores. Se han detectado lagunas en la legislación sobre protección de datos, incluso en el Reglamento General de Protección de Datos. Se requiere una orientación más adecuada sobre su interpretación y sobre la modificación de sus disposiciones. Por lo general, esas leyes se ocupan de los derechos individuales, no de las reclamaciones colectivas relativas a la privacidad, que cobrarán importancia a medida que la inteligencia artificial pase a un primer plano y, por ejemplo, un mayor número de trabajadores adopte entornos de trabajo híbridos.

97. Existe una necesidad acuciante de establecer principios comunes en materia de datos personales que puedan aplicarse a todas las leyes que prevean iniciativas de recogida de datos para hacer frente a la pandemia. Esos principios establecerían una norma común e interoperable no solo para la pandemia actual, sino también para pandemias futuras. Graham Greenleaf ha propuesto una serie de principios, que se han adaptado aquí para incluir un enfoque sobre la privacidad por diseño[62].

[62] Véase Greenleaf, "COVID-19: the available evidence … and a little bit of hindsight" (véase la nota a pie 15).

98. El mejor momento para prepararse frente a una futura pandemia es ahora[63]. Estas son enseñanzas aplicables no solo a la COVID-19, sino también a otras enfermedades transmisibles sujetas a notificación y a posibles pandemias futuras.

VIII. Recomendaciones

99. Las recomendaciones tienen por objeto garantizar el derecho de toda persona a disfrutar plenamente del derecho a la privacidad durante la presente crisis de salud pública, así como en cualquier otra crisis sanitaria futura, sin injerencias arbitrarias, como se establece en la Declaración Universal de Derechos Humanos (art. 12), el Pacto Internacional de Derechos Civiles y Políticos (art. 17) y las conclusiones de los órganos creados en virtud de tratados.

100. Las recomendaciones que figuran a continuación están dirigidas tanto a los agentes estatales como a los no estatales.

Privacidad y personalidad

101. **Los Estados y las partes no estatales deberían aplicar los Principios Rectores sobre las Empresas y los Derechos Humanos: Puesta en Práctica del Marco de las Naciones Unidas para "Proteger, Respetar y Remediar" y las directrices de género para esos Principios (A/HRC/41/43, anexo).**

102. **Adoptar las recomendaciones del Relator Especial sobre el derecho a la privacidad para la protección contra las vulneraciones de la intimidad en razón del género (A/HRC/43/52, párrs. 33 y 34)**

103. **Fomentar las asociaciones con la sociedad civil y la industria para elaborar conjuntamente estrategias y respuestas basadas en la tecnología.**

104. **Involucrar a los grupos de la comunidad en situación de especial riesgo en las consultas relativas a la adopción de medidas específicas de salud pública.**

105. **Reducir las violaciones a la privacidad por razones de género en la respuesta a la pandemia, mediante la imposición de evaluaciones del impacto en los derechos humanos respecto de la privacidad que tengan en cuenta las cuestiones de género, antes de introducir medidas, estrategias y leyes.**

106. **Evaluar periódicamente la eficacia de las medidas adoptadas para incluir a las personas en situación de vulnerabilidad y marginación en las actividades de respuesta y recuperación.**

Infancia

107. **Elaborar planes de acción integrales sobre la enseñanza en línea tomando como base el artículo 29, párrafo 1, de la Convención sobre los Derechos del Niño y las directrices del Consejo de Europa sobre la protección de datos de los niños en un entorno educativo.**

108. **Velar por que se establezcan y mantengan marcos legales apropiados para la educación en línea.**

109. **Crear infraestructuras públicas para espacios educativos y sociales no comerciales.**

[63] Véase "El mejor momento para prevenir la próxima pandemia es ahora: los países unen sus voces para mejor la preparación ante emergencias" (OMS, 1 de octubre de 2020).

110. **Velar por que los datos personales de los niños se traten de forma justa, precisa y segura, de acuerdo con una base jurídica legítima, utilizando marcos de protección de datos que representen las mejores prácticas, como el Reglamento General de Protección de Datos y el Convenio 108+.**

Privacidad de la información

111. **Integrar los derechos humanos en el diseño, la elaboración y la aplicación de estrategias tecnológicas en relación con la pandemia.**

112. **Es necesario adoptar medidas legislativas de protección basadas en principios comunes y orientadas a situaciones concretas que sean aplicables a todos los tipos de medidas sanitarias en caso de pandemia. El Relator Especial recomienda que se apliquen los 11 principios comunes [64] para los sistemas centralizados y descentralizados de vigilancia de la salud pública, las medidas legislativas para las enfermedades transmisibles y su utilización al evaluar las políticas de prevención de pandemias en todo el mundo:**

a) **Establecer la "privacidad por diseño" y "por defecto" desde el principio, mediante la incorporación de una evaluación general de los derechos humanos y de la protección de datos en las medidas de salud pública, prestando especial atención a las epidemias y pandemias[65].**

b) **La privacidad debe tenerse en cuenta desde el momento en que se pone en marcha la respuesta a cualquier epidemia o pandemia. De hecho, debería ser una piedra angular de toda estrategia nacional para hacer frente a una epidemia, estar bien concebida con años de antelación, y ser una parte integral, y bien integrada, de la evaluación general de los derechos humanos antes mencionada.**

c) **Incorporar mecanismos de control precisos y pormenorizados en la ley de protección de datos de la región o de cada país.**

d) **Proporcionar la claridad y el fundamento jurídico necesarios con una eficacia mayor que la alcanzada mediante actos delegados o reglamentos, y lograr una mayor uniformidad en la jurisdicción.**

e) **Garantizar el acceso a lugares, eventos, instalaciones, servicios educativos, etc., a fin de evitar la discriminación.**

f) **Es esencial proteger a los grupos vulnerables afectados negativamente y de forma diferenciada por las medidas de vigilancia adoptadas para combatir la pandemia.**

g) **Reducir al mínimo y definir los usos autorizados de los datos sobre la COVID a fin de garantizar que esos datos no se utilicen para otros fines una vez recopilados.**

h) **Establecer la "especificación de los fines" como en muchas leyes de protección de datos existentes.**

i) **Reducir al mínimo la recopilación de datos.**

j) **Garantizar que las medidas de recopilación de datos sean proporcionadas, establecer un enfoque de gestión de riesgos que esté**

[64] Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3875920.

[65] Véase Consejo de Europa "2020 Digital Solutions to Fight COVID-19 2020", Data Protection Report October 2020. Disponible en: www.coe.int/en/web/data-protection/-/digital-solutions-to-fight-covid-19-council-of-europe-report-on-data-protection-2020.

ampliamente aceptado y ayudar a limitar los daños causados por las filtraciones de datos, los incidentes cibernéticos y la deriva funcional.

k) **Disposiciones anticoerción. La obligación de hacer uso o de presentar una prueba de uso debe impedirse o definirse de manera rigurosa y contenida mediante la ley. Deben impedirse otras actuaciones encaminadas a exigir o requerir la presentación de certificados de uso mediante la tipificación de ese comportamiento como delito en el marco de la ley. Es preciso hacer cumplir la ley y aplicar los recursos previstos en ella.**

l) **Impedir la "infiltración de la vigilancia". Evitar que se siga el ejemplo de Singapur, que en 2020 prometió "solo rastrear" y luego se desdijo en 2021 y permitió las investigaciones penales.**

m) **La participación voluntaria que requieren la mayoría de las medidas destinadas a prevenir una pandemia precisa la confianza de la población para que funcionen. A fin de que exista esa confianza, cualquier expansión futura de las medidas de vigilancia a otras esferas, como por ejemplo, las investigaciones penales, debe ilegalizarse.**

n) **Programa de borrado continuo (si se recogen datos). La propia ley debería exigir el borrado continuo de los datos recogidos en un breve espacio de tiempo, como el periodo en el que la persona haya estado infectada o algún otro periodo de tiempo basado en datos empíricos o pruebas científicas.**

o) **La ley debe prever una "cláusula de extinción" aplicable a todo el sistema, así como la obligación de realizar una auditoría independiente del "cierre" de todos los sistemas de datos epidémicos, que deberá aplicarse con rigor. Debe establecerse un periodo fijo o una evaluación independiente de la necesidad a fin de garantizar el cierre de los sistemas de vigilancia de la pandemia, junto con la obligación impuesta por ley de realizar una auditoría independiente para comprobar que ello se ha producido.**

p) **Supervisión y presentación de informes públicos periódicos por un organismo independiente de protección de datos. La supervisión de esos sistemas de vigilancia debe ser externa e independiente.**

q) **Transparencia. Las condiciones necesarias deben definirse en consulta con los expertos y la sociedad civil. Puede consistir en la divulgación de cualquier código fuente utilizado para crear sistemas de vigilancia (como las aplicaciones de rastreo de contactos), la realización de evaluaciones exhaustivas del impacto de la protección de datos y la divulgación de datos sobre la eficacia de las técnicas utilizadas para la vigilancia de la pandemia.**

113. **Es necesario mantener un diálogo permanente con las grandes empresas tecnológicas que complemente el debate público oficial y oficioso sobre las funciones y responsabilidades que tienen esas empresas en la protección de la privacidad en caso de pandemia.**

Transparencia y medición

114. **Es preciso evaluar la necesidad y proporcionalidad de las facultades excepcionales ejercidas en situaciones de emergencia sanitaria. En el marco de esa evaluación periódica y de carácter ordinario:**

a) **El Relator Especial sobre el derecho a la privacidad, solo, así como junto con otros titulares de mandatos, debería reexaminar la situación relativa a las enfermedades sujetas a notificación y las enfermedades transmisibles, prestando especial atención a la COVID-19, aunque sin limitarse a ella, al menos**

cada 24 a 36 meses, a fin de definir los riesgos existentes y emergentes, así como para determinar cuáles son las iniciativas de política más eficaces y favorables respecto de la privacidad que puedan adoptarse para prepararse frente a posibles pandemias en el marco de un enfoque integral que proteja los derechos humanos.

b) **Si un Estado determina que es preciso aplicar medidas de vigilancia tecnológica como respuesta a la pandemia de COVID-19, debe demostrar la necesidad y la proporcionalidad de las medidas específicas y promulgar una ley que prevea tales medidas explícitamente e incluya garantías explícitas y específicas obligatorias.**

c) **Los Estados y las empresas deben incorporar los derechos humanos en el diseño, el desarrollo y la implantación de soluciones tecnológicas para hacer frente a la pandemia, dadas las importantes repercusiones que tienen las tecnologías digitales en un amplio espectro de derechos, en particular el derecho a la privacidad**[66]**.**

d) **Los Estados y las empresas deberían adoptar un diseño tecnológico centrado en el usuario que respete los derechos y permita a los viajeros llevar sus propios datos para presentarlos cuando se les solicite, como en el caso de los "pasaportes de vacunación".**

e) **Es preciso realizar un examen externo de la respuesta de los Estados ante la pandemia, así como evaluar la gestión de la pandemia por los Estados, junto con otras responsabilidades internas en materia de derechos humanos, en el marco de los exámenes periódicos que se realizan en las Naciones Unidas.**

[66] Véase A/HRC/46/19.