LOS DESAFÍOS EN TORNO A LA PRIVACIDAD Y LA VIGILANCIA EN TIEMPOS DE COVID-19

Por Bioeticar: Gricelda Moreira, Adriana Ruffa y Graciela Soifer

Gricelda Moreira

Magíster en Bioética en la Facultad Latinoamericana de Ciencias Sociales de la Ciudad de Buenos Aires (FLACSO).
Licenciada en Psicología Universidad de Buenos Aires (UBA).Psicoanalista (EFBA)
Diplomada en Bioética con orientación en reproducción asistida en la universidad Isalud, Buenos Aires.
Presidenta de Bioeticar Asociación Civil.

Adriana Ruffa

Médica especialista en Nutrición.
Secretaria de Bioeticar Asociación Civil.
Docente de Nutrición de la Facultad de Medicina de la UBA.
Miembro del Centro de Estudios y Observatorio de Bioética (CEOB) de la Universidad Isalud.

Graciela Soifer

Abogada.
Tesorera de Bioeticar Asociación Civil.
Curso de actualización en Bioética de la Facultad de Derecho (UBA).
Maestranda en Bioética FLACSO.

Desde finales del S. XIX con el fin de promover el bienestar de la población se ha desarrollado la vigilancia de la Salud Pública a nivel global.

El objetivo es contribuir a determinar patrones y causas de las enfermedades, en particular las infecciosas. Al visibilizar las problemáticas permite activar alertas, propiciar normas, como así también proporcionar los datos necesarios para la implementación de políticas adecuadas en salud pública.

La recolección de datos de vigilancia a nivel mundial sobre preparación mundial para las emergencias sanitarias generó un informe en septiembre de 2019 anticipando la posibilidad de un brote epidémico que afecte a regiones geográficas extensas.

Y es en el mes de febrero del 2020 que se declara la pandemia de COVID-19 una enfermedad infecciosa causada por el virus SARS-CoV-2 que produce síntomas similares a los de la gripe, entre los que se incluyen fiebre, tos seca, disnea, mialgia y

fatiga. En casos graves se caracteriza por producir neumonía, síndrome de dificultad respiratoria aguda, sepsias y choque séptico que conduce a cerca de 3,75 % de los infectados a la muerte según la OMS.

El organismo internacional señaló que no se trata solo de una crisis de salud pública, y que los países debían de adoptar un enfoque coordinado entre gobiernos y sociedad, construyendo una estrategia integral para prevenir infecciones, salvar vidas y minimizar el impacto y que se debía localizar, aislar, y diagnosticar cada caso de coronavirus COVID-19, siguiendo su contacto.

Al avance de la tecnología y la aplicación de grandes volúmenes de datos - Big Data- en salud, se sumaron las aplicaciones de rastreo a través de *app* instaladas en los teléfonos móviles de ciudadanos de decenas de países alrededor del mundo. Este ha sido un punto de inflexión crítico respecto a nuestros derechos y libertades, y a los desafíos que se presentan en torno a la privacidad y la vigilancia en tiempos de COVID-19.

Vigilancia en Salud Pública

En un principio cuando a se comenzaron a realizar los informes para la Vigilancia-finales del siglo XIX- eran elaborados por médicos y los datos se utilizaban para dejar constancia de los avances de una enfermedad. Más adelante la información permitió intervenir a nivel personal a partir de la determinación de que los gérmenes se transmiten persona a persona. Si bien dichas intervenciones permitieron derivar a las personas a una consulta o proveerles ropa y alimento, también permitió imponer tratamientos, cuarentenas y hasta deportación.

Desarrollaremos en éste acápite el informe sobre la Vigilancia en Salud desarrollado por la OMS[65], donde se la define como la recolección, el análisis y la interpretación sistemáticos y continuos de datos de salud con el fin de planificar, analizar y evaluar las prácticas en esa esfera.

No realizar la vigilancia por parte de los Estados podría evitar dejar registro de lo que acontece, incluyendo las desigualdades e inequidades en el acceso a la salud.

Sin embargo, realizar la vigilancia sin considerar los efectos posibles de estigmatización, discriminación incluso de prolongación de la inequidad, es controversial, en especial si la definición de la vigilancia de la salud pública difiere de un país a otro, y no se confía en el resguardo de la confidencialidad de la información.

En este punto es importante interrogarnos respecto a los marcos éticos específicos para la vigilancia. La búsqueda nos confronta conun vacío en pautas internacionales como

[65]Selgelid MJ. Public Health: VII. Health Surveillance. En: Jennings B, Editor. Bioethics. 4ta ed, Farmington Hills, MI: Macmillan; 2014. p. 2635–2639 citado en Pautas de la OMS sobre la ética en la vigilancia de la salud pública https://iris.paho.org/handle/10665.2/34499 consultado el 25 de mayo 2020.

lo ha señalado el Consejo de Organizaciones Internacionales de las Ciencias médicas (CIOMS)[66].

Se entiende por datos de salud a todas las enfermedades no transmisibles como transmisibles, estas últimas pueden implicar una propagación en diferentes países y al respecto se ha elaborado en el año 2005 un Reglamento Sanitario Internacional (RSI) que define la vigilancia como "*la compilación, comparación y análisis de datos de forma sistemática y continua para fines relacionados con la salud pública, y la difusión oportuna, para su evaluación y para dar la respuesta de salud pública que sea procedente*"[67]. Si bien en un inicio, en los años setenta este reglamento se había enfocado en las enfermedades transmisibles, cuando se realizó la revisión hace quince años, se amplió a cualquier enfermedad que constituya una emergencia a nivel internacional.

El reglamento se limita a imponer la obligación a los Estados Miembros de prevenir la expansión de una enfermedad, a través de la recolección de datos y de vigilancia. Pero esto no implica que se cuente con instrumentos para abordar éticamente el problema que generan los sistemas de vigilancia.

Es claro que, en la puesta en marcha de este recurso, el objetivo deberá ser no causar daño a las personas teniendo en cuenta que puede limitar la privacidad y otras libertades civiles.

La vigilancia en contextos disímiles, con estructuras políticas, sociales y económicas muy distintas, puede ser utilizada para violar los derechos de las personas, su autonomía y su confidencialidad, provocando mayor inequidad e injusticia.

¿Qué seguridad tenemos que la vigilancia no se transforme en un castigo o un privilegio? Generar pautas éticas, es un buen principio sin duda. La OMS ha propiciado tres iniciativas para la elaboración de pautas éticas en el control de las enfermedades. Si bien, enfatizan la equidad, la justicia y el bien común, hay algunos puntos que no son sencillos de resolver como los daños económicos, legales, psicológicos, sociales o físicos. Por ello la importancia de garantizar la seguridad de los datos a partir de medidas operativas y tecnológicas para prevenir la divulgación.

Sin embargo, no podemos desconocer que la seguridad no es infalible, y quien se encarga de recolectar datos de vigilancia debe hacerse responsable de protegerlos con la máxima rigurosidad.

---

[66]Pautas éticas internacionales para la investigación relacionada con la salud con seres humanos, Cuarta Edición. Ginebra: Consejo de Organizaciones Internacionales de las Ciencias Médicas (CIOMS); 2016. https://cioms.ch/wp-content/uploads/2017/12/CIOMS-EthicalGuideline_SP_INTERIOR-FINAL.pdf consultado el 25 de mayo 2020

[67]Reglamento Sanitario Internacional (2005). Segunda edición, Ginebra, Organización Mundial de la Salud, 2008, disponible en http://www.who.int/ihr/IHR_2005_es. Consultado el 25 de mayo 2020

Si bien el consentimiento informado-CI-ha adquirido preponderancia en los últimos años a partir de considerar la autonomía un principio rector, lo cierto es que la vigilancia en salud pública no tiene como norma exigir el consentimiento por la falta de factibilidad y por considerarlo injustificado cuando los riesgos son bajos, todo esto respaldado por las normas CIOMS. Y en los casos en el que se solicita el CI deberá cumplir con ciertas condiciones para que sea garantizada la voluntariedad.

Por el bien común es importante colaborar con la información y hasta moralmente necesario, pero el informe de la OMS enfatiza que es imprescindible garantizar la no difusión con organismos o con propósitos no relacionados con la salud pública.

En situaciones de emergencia, el acceso a la información de manera rápida y éticamente adecuada es fundamental para contar con la posibilidad de dar respuesta por parte del sistema de salud. El compartir datos es algo estipulado en el RSI y una obligación en el caso de enfermedades infecciosas.

En lo que respecta a la vigilancia, se dieron importantes adelantos al momento de recolectar y compartir datos desde las redes sociales o los datos de geolocalización a partir de la telefonía móvil e identificar enfermedades infecciosas como genéticas, pudiendo predecir los movimientos de las personas y los contactos con otros, armando un mapa de la propagación de enfermedades.

A partir del año 2005 se implementa el término *Big Data* como expresión de una nueva fase del paradigma intensivo en información y comunicación.

Shoshana Zuboff[68] (2015) asegura que la dificultad de concebir una definición de '*big data*' tiene que ver con que todavía se piensa como un objeto estrictamente tecnológico. Esta académica argumenta que, por encima de su carácter técnico, se trata de un componente intencional que emerge como consecuencia de la nueva lógica de acumulación de lo que denomina 'capitalismo de vigilancia', una nueva forma de capitalismo informacional que aspira a predecir y modificar la conducta humana para producir ganancias y control de mercados.[69]

En el caso de la salud, los datos digitales pueden originarse a partir de registros médicos electrónicos e imágenes, aunque también pueden considerarse datos farmacológicos, ambientales y hábitos de los pacientes, entre otros. De esta manera, *Big Data* permitiría mejorar la capacidad de respuesta del sistema de salud pública, incrementar la detección temprana de enfermedades y reducir los tiempos de investigación médica, o bien, avanzar hacia una medicina personalizada utilizando los datos de pacientes.

En el campo sanitario la difusión y el cruce de información en la web entraña riesgos que se vinculan directamente con derechos fundamentales de las personas. El

[68]Shoshana Zuboff es socióloga, profesora emérita en Harvard y escritor estadunidense. Algunos de los temas más recurrentes en sus obras son la revolución digital la evolución del capitalismo la emergencia histórica de la individualidad psicológica y las condiciones del desarrollo humano.
[69]https://www.vialibre.org.ar/wp-content/uploads/2019/11/B.Busaniche.-Transparencia-Vigilancia-Y-Control-Social.pdf consultado 7/6/20

conjunto de datos sensibles almacenados puede usarse tanto para mejorar la atención a los pacientes como para direccionar publicidad y hasta discriminar a personas con determinadas patologías.

El buscador Google, que realiza el 68% de las búsquedas de Internet en los Estados Unidos y el 90% en Europa, reconoce que una de cada cinco búsquedas de información en línea se vincula con la salud. Así parecen estar abriéndose las puertas para que compañías de marketing que diseñan avisos específicos para el usuario o empresas dedicadas al almacenamiento de datos puedan recoger información sensible para luego comercializarla.

Este nuevo contexto en el ámbito sanitario requiere ser analizado críticamente a fin de poder proponer medidas firmes y consistentes de protección de datos. La anonimización ha sido hasta ahora la condición necesaria que permitía cumplir con las normas de protección de los datos personales. Se sostiene que un conjunto de datos personales, al ser anonimizados, dejan de contener información sensible y quedan por afuera de la protección legal. Sin embargo, debemos reconocer que mediante el uso de técnicas de ingeniería informática es posible cruzar datos e identificar a la persona a quien pertenecen, volviendo obsoletas las medidas de resguardo del anonimato.

El tratamiento de uso masivo de datos –*Big Data*- relacionados con la salud plantea serios interrogantes que es necesario debatir con transparencia y la necesaria participación democrática. ¿Quiénes pueden acceder a esos datos? ¿Quién garantiza que las empresas desarrolladoras o las que comercializan no acceden, comparten o venden esa información? Y una vez volcados los datos en la *app* generada por parte del Estado ¿quién puede acceder a ellos? ¿Para qué? ¿Qué uso sería éticamente justificado? ¿Cuánto tiempo debe guardarse la información? ¿Puede garantizarse la privacidad, la confidencialidad y veracidad de la información?[70]

Los beneficios que el *Big Data* puede tener para la salud de las personas, tanto porque facilita información sobre su conducta y eso ayuda en el diagnóstico y la adhesión a los tratamientos, como por el impulso que supone para la investigación y la innovación disponer de infinidad de datos relacionados con la salud y la enfermedad, son indudables. Pero al mismo tiempo se advierte que el manejo de toda esa información exige un marco ético y jurídico que permita conocer cómo se gestionan los beneficios que se obtengan para la investigación, para qué y para quién se investiga y quién ejerce el control presente y futuro.

A su vez, las formas de otorgamiento del consentimiento informado como expresión de la autonomía de los pacientes frente a los desafíos que se presentan ante estos cambios en el tratamiento de los datos vinculados a la salud deberán ser revisados, por la complejidad y variedad de matices que aparecen con el uso de la información

[70] Bioeticar: "De la Historia clínica al Big Data" en el Anuario de Bioética y Derechos Humanos del Instituto Internacional de Derechos Humanos (IIDHA) Capítulo para las Américas 2017 pág. 48 a 69 http://www.bioeticar.com.ar/assets/pdf/anuario_bioetica_y_ddhh.pdf

Los macrodatos se presentan como una oportunidad para la vigilancia en salud pública, debido a que pueden vincularse directamente con los registros sanitarios o historias clínicas electrónicas. Pudiéndose utilizar datos de salud pública para alimentar sistemas automáticos para activar alertas y advertencias en salud, incluyendo los datos de geolocalización a través de los teléfonos celulares, detectando los movimientos de las personas y la propagación de la enfermedad.

"Por un lado, la vigilancia permite a las intervenciones de salud pública abordar las inequidades. Por otro lado, la vigilancia puede usarse para imponer cargas adicionales sobre aquellos que están ya en situación de desventaja. La única seguridad de que la vigilancia no se convertirá ni en privilegio ni en castigo es prestar atención a las consideraciones éticas: tanto las cargas como los beneficios deben sopesarse mediante un análisis crítico y luego distribuirse de una manera justa y transparente, tarea de la cual los Estados han de rendir cuentas."

La recolección de datos de vigilancia a nivel mundial generó el informe anual[71] sobre preparación mundial para las emergencias sanitarias. Las Naciones Unidas y la OMS consideran que la *preparación*[72] implica introducir mecanismos que permitan a las autoridades nacionales, las organizaciones multilaterales y las organizaciones de socorro humanitario detectar los riesgos y desplegar personal y recursos con rapidez cuando se produce una crisis.

En el mes de septiembre de 2019, la Junta de Vigilancia Mundial de la Preparación[73] exhortó a los jefes de gobierno de todos los países a comprometerse en virtud del Reglamento Sanitario Internacional (RSI (2005) a dedicar una partida prioritaria de los recursos y los gastos ordinarios, a la preparación ante una emergencia y a construir sistemas sólidos que generen confianza, dando prioridad a la participación de la comunidad a múltiples partes interesadas - tanto legisladores, representantes de los sectores de la salud humana y animal, la seguridad y los asuntos extranjeros; el sector privado; los dirigentes locales; las mujeres y la juventud-.

En dicho informe un acápite señala lo siguiente: que el mundo corre grave peligro de padecer epidemias o pandemias de alcance regional o mundial y de consecuencias devastadoras, no solo en términos de pérdida de vidas humanas sino de desestabilización económica y caos social. Asimismo, refiere "*Aumentan las probabilidades de que se*

[71]Junta de Vigilancia Mundial de la Preparación. Un mundo en peligro: informe anual sobre preparación mundial para las emergencias sanitarias. Ginebra, Organización Mundial de la Salud, 2019.https://apps.who.int/gpmb/assets/annual_report/GPMB_Annual_Report_Spanish.pdfconsultado el 25 de mayo 2020

[72] What is preparedness? En: Humanitarian response [sitio web]. Nueva York, Oficina de Coordinación de Asuntos Humanitarios de las Naciones Unidas, 2019 https://www.humanitarianresponse.info/en/coordination/preparedness/what-preparednessconsultado el 25 de mayo 2020.

[73] La Junta, cofundada en mayo de 2018 por el Grupo del Banco Mundial y la Organización Mundial de la Salud, está integrada por 15 miembros, participan dirigentes políticos, jefes de organismos y expertos, bajo la coordinación de la Dra. Gro Harlem Brundtland, ex Primera Ministra de Noruega y ex Directora General de la Organización Mundial de la Salud, y el Sr. Elhadj As Sy, Secretario General de la Federación Internacional de Sociedades de la Cruz Roja. Los miembros participan en la Junta a título personal.

declare una pandemia a escala mundial. Si bien los avances científicos y tecnológicos ofrecen nuevos instrumentos para promover la salud pública (lo que incluye efectuar una evaluación segura de las contramedidas médicas), también permiten la creación o recreación en laboratorio de microorganismos que pueden causar enfermedades. Una liberación intencionada complicaría la respuesta al brote epidémico resultante, ya que, además de decidir la forma de luchar contra el patógeno, habría que introducir medidas de seguridad que limitarían el intercambio de información y fomentarían las divisiones sociales. En conjunto, los eventos naturales, accidentales o intencionados causados por patógenos respiratorios de gran impacto plantean «riesgos biológicos catastróficos a escala mundial»[74]

El contexto actual se caracteriza por la pérdida de confianza en los gobernantes, los medios de comunicación, los sistemas sanitarios, y la difusión de falsas noticias que circulan a través de las redes y que se difunden con extrema rapidez.

El documento manifestaba que "*Los sistemas y capacidades existentes en materia de preparación y respuesta ante brotes epidemiológicos son insuficientes para hacer frente a la enorme repercusión y rápida propagación de una pandemia altamente mortífera, ya fuera de origen natural o liberada accidental o intencionadamente, así como a la conmoción que supondría para los sistemas sanitarios, sociales y económicos"*

Además, se registrauna ausencia de planes integrales de movilización de recursos, con cálculo de costos, para apoyar la preparación en caso de emergencias sanitarias en los sistemas de salud, la salud humana, la salud animal, la gestión de desastres y el medio ambiente.

La pandemia anunciada

El 11 de marzo de 2020 el director general de la Organización Mundial de la Salud (OMS), Tedros Adhanom Ghebreyesus, declaró que el coronavirus Covid-19[75] pasa de ser una epidemia a una pandemia. Señalando que no se trata solo una crisis de salud pública, y que los países debían de adoptar un enfoque coordinado entre gobiernos y sociedad, construyendo una estrategia integral para prevenir infecciones, salvar vidas y minimizar el impacto y que se debía localizar, aislar, y diagnosticar cada caso de coronavirus Covid-19, siguiendo su contacto.

Desde aquel entonces, infinitos esfuerzos se han hecho para prevenir, atender y procurar mitigar la propagación de la enfermedad y su impacto sobre los sistemas

[74]Schoch-Spana M, Cicero A, Adalja A, Gronvall G, Sell TK, Meyer D et al. Global catastrophic biological risks: toward a working definition. Health Security. 2017;15(4):323–8 citado en GPMB_Annual_Report_Spanish.pdf

[75] La COVID-19 (acrónimo del inglés *coronavirus disease 2019*), es una enfermedad infecciosa causada por el virus SARS-CoV-2. Produce síntomas similares a los de la gripe, entre los que se incluyen fiebre, tos seca, disnea, mialgia y fatiga. En casos graves se caracteriza por producir neumonía, síndrome de dificultad respiratoria aguda, sepsias y choque séptico que conduce a cerca de 3,75 % de los infectados a la muerte según la OMS. No existe tratamiento específico; las medidas terapéuticas principales consisten en aliviar los síntomas y mantener las funciones vitales.

sanitarios. En todos los países se tomaron medidas que intentaron buscar un equilibrio entre la protección de la salud, la minimización de los trastornos sociales y económicos y el respeto de los Derechos Humanos.

En ese hacer la tecnología irrumpió como un aliado para combatir la pandemia implementándose sofisticados sistemas de vigilancia para controlar los movimientos de las personas infectadas, establecer las cuarentenas, identificar posibles portadores mediante sensores de temperatura y geolocalizadores y regular los permisos de circulación, entre otros.

Al momento de escribir este texto, más de 18 millones de personas en todo el mundo se han contagiado del nuevo coronavirus, el cual ha provocado ya la muerte de 692.000 personas. La incidencia del COVID-19 es diferente en cada país y dentro de cada uno, por lo que las medidas deben ser específicas en cada lugar. Lo cual ha generado modos diferentes de encarar la crisis sanitaria por los diferentes Estados.

Una de las medidas tomadas ha sido la necesidad de distanciamiento social por parte de las personas para evitar la propagación del virus, de ese modo se ha puesto en suspenso el derecho de asociación en pos del bien común.

Por otro lado, la tecnología ofrece la posibilidad de rastrear y contactar a quienes han estado potencialmente expuestas al COVID-19 y a través de señales de bluetooth determinar qué tan cerca ha estado de los pacientes diagnosticados con el virus. La creación de las *apps* se integra a los sistemas operativos iOS y Android, se intenta que la recopilación de datos se minimicesolo a cuestiones de salud por parte de las autoridades sanitarias, deben obtener el consentimiento del usuario y un segundo consentimiento antes de compartir los resultados de las pruebas con las autoridades de salud pública, como un intento de evitar abusos y salvaguardar la privacidad del usuario. Muchos gobiernos consideran clave el uso de estas *apps* para frenar los contagios.

China es un ejemplo extremo en el control que llevó adelante con medidas tecnológicas intrusivas, la aplicación contaba con un código QR que detectaba las zonas donde había circulado la persona, si la zona era segura el código era verde y si ingresaba a zonas inseguras el color era rojo y esos ciudadanos no podían ingresar a los medios de transporte público, oficinas o residencias.

Los países asiáticos consideran que la vigilancia digital a través de *big data* puede ayudarlos a salvar vidas. En China la vida de sus ciudadanos está bajo control mucho antes del surgimiento del virus, existe un intercambio de información entre la telefonía móvil y las autoridades y pueden acceder a viajes u otros beneficios más económicos a partir de una evaluación de cada uno de ellos- desde si cruzan o no un semáforo en rojo, hasta los comentarios en redes-, también cuentan con más de 200 millones de cámaras de vigilancia de inteligencia artificial. Lograron contener la epidemia a través de su infraestructura de control y por la falta de conciencia crítica ante la vigilancia digital. Al decir del filósofo

surcoreano Byung Chul Han se implementa una biopolítica digital que acompaña a la psicopolítica digital que controla activamente a las personas.[76]

En Corea del Sur, se han publicado detalles muy específicos sobre individuos infectados. Israel se plantea usar al servicio secreto para vigilar a los ciudadanos a través de sus móviles. En Estados Unidos, el Gobierno discute con las grandes tecnológicas desarrollar medidas similares.

En España están ofreciendo al Gobierno controlar los movimientos de las personas que están en cuarentena. Coronamadrid[77], por ejemplo, no permite uso anónimo, no pide consentimiento, no establece periodo de retención de datos, no minimiza datos, y comparte datos médicos sin anonimización.

Para John Scott Railton, investigador del Citizen Lab, de la Universidad de Toronto, "muchos sectores, ya sea compañías de anuncios o de teléfonos están recolectando esos datos sobre dónde ha estado la gente y esta información parece ser una herramienta prometedora para cosas como rastrear los recorridos de las personas, saber si se quedan en casa, entender si las personas a las que se les ha ordenado estar en aislamiento lo cumplen. Y más allá de todo, saber si la gente ha tenido o no contacto con otros.

Para la vuelta a la normalidad post pandemia no son pocas las voces que proponen adoptar un carnet o pasaporte de inmunidad, que en la práctica se trataría de un certificado, una pulsera identificativa de colores o un código QR para permitir que las personas con anticuerpos puedan realizar actividades que en principio no podrían llevar a cabo el resto.

Con relación a esta última propuesta adelantamos nuestra posición de absoluto rechazo. La idea de exigir un pasaporte de inmunidad para controlar el acceso de personas a lugares o trabajos es una medida claramente desproporcionada y discriminatoria. Tal como sostiene Ianza Itziar de Lecuona, profesora del Departamento de Medicina y subdirectora del Observatorio de Bioética y Derecho de la Universidad de Barcelona, "desde el punto de vista de la bioética, es estigmatizador, no respeta la autonomía de las personas y generaría una situación de desigualdad".

Por otra parte, considerando el actual conocimiento que se tiene de la etiología del SARS-CoV-2, tampoco se justificaría la medida. "Todavía no sabemos ni siquiera cuánto dura la inmunidad tras haber pasado el virus, y la serología tiene posibilidad de dar falsos positivos y falsos negativos". [78]

Argentina y el COVID 19

[76]Byung Chul Han: "El virus no puede reemplazar a la razón"

[77] Página web y app permiten a sus usuarios la geolocalización, siempre que activen esta funcionalidad, con el objetivo de organizar mejor los recursos sanitarios para lograr una respuesta más ágil y eficaz en cada caso particular. https://www.redaccionmedica.com/autonomias/madrid/coronavirus-madrid-lanza-la-app-coronamadrid-para-diagnosticar-contagios-4958

[78] Padilla, J &Gullón,P (2020) *Epidemiocracia.* Madrid: Capitan Swing

En Argentina la aplicación tecnológica se denomina “Cuidar”, tiene valor de declaración jurada y falsear la información puede considerarse una contravención grave, el ciudadano debe ingresar sus datos personales para que pueda realizarse un seguimiento, el escaneo de su documento nacional de identidad, el domicilio en el que se encuentra realizando el aislamiento, el número de teléfono y luego se habilita la geolocalización. A partir de la incorporación de esos datos, debe ingresar temperatura y responder cuatro preguntas relacionadas con los síntomas de covid19. También debe completar datos vinculado a estados de salud- diabetes, enfermedad hepática, renal crónica, respiratoria o cardiológica, cáncer-. Al concluir el proceso en caso de no tener síntomas se genera un certificado emitido por el Ministerio de Salud que lo autoriza a ir a trabajar los próximos 14 días.

En nuestro país a la prórroga de la emergencia sanitaria por la pandemia se sumó el aislamiento social, preventivo y obligatorio, por un plazo determinado, durante el cual todas las personas debieron permanecer en sus residencias habituales o en el lugar en que se encuentren y abstenerse de concurrir a sus lugares de trabajo.

Dichas medidas se complementaron con la implementación de la aplicación denominada Cuidar COVID -19 en su versión para dispositivos móviles. En un principio se dispuso su uso obligatorio para toda persona que hubiera ingresado al país, descargable en forma gratuita de las tiendas de aplicaciones o en su versión web accesible a través de un sitio web oficial. Luego se promovió su uso para circular dentro del país y tuvo como función principal indagar sobre síntomas de los ciudadanos y rastrear pacientes con coronavirus a partir de la geolocalización.

La pregunta que surge es si entregar nuestros datos personales es el mecanismo para frenar el contagio del virus. Lo que es seguro es que resulta un método invasivo a nuestra privacidad y autonomía, pero no necesariamente fiable en el control de la pandemia.

En particular porque este sistema deja por fuera a todos los asintomáticos que seguirán pululando y contagiando con un certificado expedido por el propio Ministerio de Salud. Las personas asintomáticas juegan un rol fundamental en el contagio, un claro ejemplo es el que obtuvo la Universidad de Padua en Italia, cuando el pueblo de Vo sufrió la primera muerte por covid19 y se realizaron pruebas a todos sus habitantes y descubrieron que muchos de los que dieron positivo no padecían síntoma alguno.[79]Al respecto el médico de la Universidad de Florencia Sergio Romagnani comenta que el resultado que se obtuvo de los test aplicados sobre una muestra muy pequeña, pero aun así es muy revelador. Un total de 58 personas dieron positivo en las pruebas realizados entre el 22 y el 25 de febrero y, de todos ellos, 33 eran totalmente asintomáticos, la mayoría de estos era menor de cincuenta años. Surgiendo la hipótesis de que entre el 50 % y el 70 % de los infectados no estarían desarrollando síntomas.

[79]https://www.semana.com/mundo/articulo/pueblo-en-italia-controlo-el-coronavirus-haciendo-pruebas-a-todos-e-ignorando-la-oms/663038

Para la investigadora Carissa Véliz[80] la opción de recurrir a *apps* no solo es más invasiva desde el punto de vista de la privacidad, sino también mucho menos preciso y efectivo.Didier Raoult, especialista francés en enfermedades infecciosas, considera que hay que hacer pruebas a toda la población y priorizar el diagnóstico. Haciendo pruebas solamente a quienes terminan en el hospital habrá una mayoría de gente infectada que se detecta demasiado tarde, ya con síntomas y habiendo contagiado a otros.

Por otro lado, es pertinente considerar el riesgo que este tipo de sistemas de vigilancia continúen cuando la pandemia haya cesado. Los Estados parecen haber encontrado una vía regia para incorporar el control de sus ciudadanos, mientras -que en esta ocasión- son las empresas como Apple y Google[81] quienes han intentado poner freno a los excesos prohibiendo el uso de rastreo de ubicación lo que complicaría el uso de muchas de las *apps* descriptas anteriormente y diseñada por los Estados para ubicar a las personas sobre la posible exposición a COVID-19. Asimismo, dichas empresas establecen que los datos deben permanecer descentralizados de cada teléfono, que las *apps* no pueden ser obligatorias, que deben ofrecer diferentes tipos de consentimientos a sus usuarios, y que la información se autodestruya a los 14 o 21 días.

La privacidad y el COVID-19

Según el Diccionario de la lengua de la Real Academia Española, «privacidad» se define como el ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión.

Sin duda, el concepto de privacidad no es unívoco. Aparece en los debates sobre las escuchas telefónicas, los derechos sexuales y reproductivos, los deberes de los profesionales de la salud, la correspondencia epistolar, las TICs, el enfoque de género, los mercados digitales y financieros, el ciberdelito y un gran número de otros escenarios.

La privacidad y la confidencialidad pueden considerarse parte del derecho a la intimidad de las personas como derecho fundamental. No se trata de un derecho nuevo en él sino es un derecho consagrado como Derecho Humano y reconocido tanto en el orden constitucional de muchos países como en tratados universales y regionales de Derechos Humanos.

Desde la Declaración Universal de los Derechos Humanos de 1948 que manifiesta en el artículo 12 "*Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques*", la garantía se ha mantenido incuestionable y reiterada.

[80]Carissa Véliz es investigadora en el Uehiro Centre for Practical Ethics y el Wellcome Centre for Ethics and Humanities de la Universidad de Oxford

[81]https://www.technologyreview.es/s/12196/google-y-apple-prohiben-captar-la-ubicacion-en-su-app-de-rastreo-de-contactos

Sin embargo, es durante la última parte del siglo XX y el siglo actual donde la privacidad en un mundo globalizado ha cobrado nueva relevancia. En palabras de la académica Shoshana Zuboff, los datos recogidos en forma permanente de todas y cada una de nuestras interacciones sociales mediadas por tecnologías de información y comunicación constituyen el insumo fundamental de una industria que desarrolla sistemas que de formas más o menos precisas permiten no sólo prever nuestras conductas, sino y fundamentalmente amoldarlas a los intereses económicos que las sustentan.

Shoshana Zuboff, advierte sobre una nueva forma de inequidad, la "desigualdad epistémica". El mejor ejemplo de esto es la abismal diferencia entre lo poco que sabemos sobre estas empresas y todo lo que ellas saben de nosotros.

Por otra parte, más allá de qué es lo que "queremos mantener privado", lo importante es que esa voluntad siempre depende de un contexto. En efecto, como dice Helen Nissenbaum[82] en su libro "Privacidad amenazada"[83], una acción o práctica viola nuestra privacidad en función del contexto en el cual la actividad tiene lugar y también según cuál sea el tipo de información en cuestión y los roles sociales en los que las personas están inmersos. Los contextos sociales, tales como los de los servicios de la salud, la educación, el comercio y la religión, se rigen por normas sociales complejas y relaciones de poder.

De acuerdo a la integridad contextual definida por Nissenbaum, en un contexto de amistad, los amigos comparten informaciones, no por obligación, sino por propia decisión. Fuera de ese contexto, esas informaciones tienen otro peso y valor. El problema es que hoy las tecnologías de la información y las redes sociales permiten que esa información se descontextualice, no solo sin nuestro consentimiento sino casi inadvertidamente para la mayoría. Podemos creer que estamos hablando en privado con amigos en Facebook, sin embargo en algún lugar habrá procesadores que mediante algoritmos analizan nuestras palabras para encontrar información de valor comercial, definir nuestros perfiles de gustos e intereses y también organismos estatales tratando de detectar actividad potencialmente sospechosa para la seguridad.

Si estos riesgos los trasladamos a un contexto de crisis y pandemia aparecen nuevos interrogantes y riesgos sobre la biovigilancia, que se ha adueñado de tecnologías desarrolladas originalmente para otros propósitos.

El concepto de habeas data, protección de datos y el COVID-19

Habeas data es un término latino que significa "tienes tus datos", "tened la información o los datos". Se trata de una garantía constitucional que permite a las personas pedir explicaciones a los organismos públicos o privados que poseen datos o información

[82]Helen Nissenbaum es profesora de ciencias de la información en Cornell Tech. Conocida por el concepto de "integridad contextual" y su trabajo sobre privacidad, leyes de privacidad, confianza y seguridad en el mundo en línea.
[83]Nissenbaum , H. (2012), Privacidad amenazada: Tecnología, política y la integridad de la vida social, Buenos Aires: Océano.

sobre ellas, y así averiguar qué datos tiene, cómo los han obtenido, por qué y para qué los tienen.

Esta garantía encuentra su fundamento en el artículo 19 de la Constitución Nacional y se incorporó explícitamente en la Carta Magna con la reforma de 1994, en el artículo 43, 3º párrafo, al otorgar la acción de amparo a toda persona que requiera *tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos.* Así se consagró el derecho de a rectificar la información que tanto el Estado como entidades privadas posean sobre las personas.

En el año 2000 se sancionó la ley 25.326 de protección de datos personales, que establece un claro encuadre jurídico para el tratamiento de información referida a la salud, entre otros datos sensibles, teniendo en cuenta que se trata de una actividad que debe llevarse adelante con especial cuidado, respetando la privacidad de las personas. (Conf. Arts. 2 y 7 ley 25.326.)

El objeto general de la norma es proteger el derecho a la intimidad y a la privacidad, que incluye el resguardo a la divulgación de información sensible de las personas.Se entiende por "datos sensibles" aquellos que revelan origen racial y étnico, los referentes a los referentes a opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

Dentro de este encuadre legal la divulgación del nombre de un paciente que padezca de coronavirus requiere de su consentimiento. Los establecimientos sanitarios y los profesionales de la salud pueden procesar y cederse entre sí datos de los pacientes, siempre y cuando cumplan con el secreto profesional y estén anonimizados.

En cuanto a la obligación de secreto profesional subsistirá aun después de finalizada la relación con el paciente. Para usar la información del paciente con fines incompatibles con su tratamiento médico, se debe requerir su consentimiento pleno, libre e informado.

El Ministerio de Salud de la Nación y los ministerios provinciales se encuentran facultados a requerir, recolectar, cederse entre sí o procesar de cualquier otro modo información de salud sin consentimiento de los pacientes, conforme a las competencias explícitas e implícitas que les hayan sido conferidas por ley. Es decir solo si se recaban para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal (art. 5, inc. 2 b) y se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias. (Art. 11, inc. 3 b)

Reiteramos el rastreo de contactos es un componente importante de una respuesta eficaz a la pandemia y las aplicaciones de rastreo de contactos pueden ser de utilidad con tal fin. Pero, para que sean compatibles con los derechos humanos y con nuestro ordenamiento legal tales aplicaciones deben, entre otras cosas, incorporar en su diseño la

protección de los datos y la privacidad, lo que significa que los datos recopilados deben ser los mínimos necesarios y almacenarse de forma segura.

Además, toda recopilación de datos debe limitarse al control de la propagación de la COVID-19 y no servir a ningún otro propósito, como hacer cumplir la ley, velar por la seguridad nacional o controlar la inmigración. Tampoco debe ponerse a disposición de terceros ni destinarse a fines comerciales. Además, la decisión individual de descargar y usar aplicaciones de rastreo de contactos debe ser completamente voluntaria y debe protegerse la confidencialidad de todos los datos recopilados, incluso si se combinan con otros conjuntos de datos.

Reflexiones finales

Los estados estaban advertidos, al inicio de este trabajo nos referimos al informe anual sobre preparación mundial para las emergencias sanitariasllevado adelante por la Junta de Vigilancia Mundial de la Preparación e informada por la OMS en septiembre de 2019[84].

Como parte de los preparativos que los países deben llevar adelante antes de que se declare una pandemia, es examinar sus leyes, sus políticas respecto al tratamiento que se haga de la información personal, y tomar las medidas necesarias para proteger el bien común y respetar la privacidad y autonomía de sus ciudadanos. Así cómo también evitar el acceso a la información a cualquier otro organismo del estado o privado, todo lo cual puede infligir mayor daño y vulnerabilidad.

Yuval Noah Harari[85] advirtió en un artículo publicado en el Financial Times: "*Muchas medidas de corto plazo tomadas durante la emergencia se convertirán en parte integral de la vida. Esa es la naturaleza de las emergencias, aceleran los procesos históricos. Decisiones que en tiempos normales llevarían años de deliberación se aprueban en cuestión de horas".* El historiador israelí cree que nos enfrentamos al dilema entre vigilancia totalitaria y empoderamiento ciudadano.

El binomio público-privado en una sociedad democrática comprendido entre el derecho a la privacidad, como derecho individual y personalísimo entra en tensión con las necesidades de la salud pública, entendida como bien colectivo.

O dicho de otro modo se nos presenta un escenario de límites imprecisos entre los derechos individuales y los derechos de la sociedad, terreno históricamente conflictivo y marcado por ideologías y tesis contrapuestas sobre el alcance y el rol del Estado.

Desde la Bioética con un enfoque de derechos humanos y el aporte que desde la filosofía kantiana, con su defensa de la persona como un fin en sí mismo y nunca como un

[84]https://apps.who.int/gpmb/assets/annual_report/GPMB_Annual_Report_Spanish.pdf
[85]Yuval Noah Harari es un historiador y escritor israelí, profesor en la Universidad Hebrea de Jerusalén. Entre sus obras se encuentran Sapiens: De animales a dioses, Homo Deus: Breve historia del mañana y 21 lecciones para el siglo XXI

medio, por más loable que este sea, nos interpelamos sobre la necesidad de intentar establecer los alcances y la razonabilidad de las posiciones en juego.

Es necesario contar con un plan de contingencias que ante la emergencia se ponga en funcionamiento, pero nada será más importante que contar de antemano con un sistema sanitario en funcionamiento y un estándar alto de pautas éticas previamente elaborado.