La herejía *tecno-optimista* florece en pandemia

Un repaso crítico a las tecnologías disponibles

María Paz Canales

DERECHOS DIGITALES
América Latina

La herejía *tecno-optimista* florece en pandemia

Un repaso crítico a las tecnologías disponibles

María Paz Canales

Texto por María Paz Canales.
Edición por Vladimir Garay.
Diseño y diagramación por Constanza Figueroa.

Los íconos “Apps” de Bin Hur, “Network” de Josh Sorosky, “Diagnose” de jeehan@design, “Decision making” de Chrystina Angeline, “Passport” de Chanut is Industries, “Surveillance” de Max Hancock, “Location” de Adrien Coquet y “Virus” de mim studio, utilizados en el diseño de esta publicación, son parte de The Noun Project.

Junio de 2020

ÍNDICE

Mientras escribo estas líneas desde la comodidad y privilegio de mi confinamiento, en Chile se registran 174.293 contagios y 3.323 fallecidos, y cada minuto muere un brasilero a causa de una infección por Coronavirus. En el mundo ya se totalizan más de siete millones de contagiados. América registra el mayor número de contagios en el mundo, con Estados Unidos y Brasil dentro de las tres naciones con mayor número de infectados, y más de 150.000 muertos en total. En Chile, el gobierno organiza la llegada de canastas básicas de alimentación a la población luego de volver a extender por otra semana el confinamiento total en el área metropolitana y otras provincias del país. Semanas atrás, se desplegó en uno de los edificios más altos y simbólicos de la ciudad de Santiago el mensaje HAMBRE.[1]

El miedo, se ha dicho siempre, es mal consejero. En las circunstancias actuales, el miedo al hambre y el miedo a la muerte es real y tangible, más todavía en una América Latina carente de redes de protección social que aseguren a quienes no pueden salir a trabajar que recibirán el apoyo que les permita alimentarse y alimentar a sus familias, al menos hasta que sea seguro volver a salir. La combinación de una pandemia con economías precarias, que viven al día, y servicios de salud en los cuales se ha invertido escasamente, son los ingredientes para una tormenta perfecta.

La herejía tecno-optimista encuentra terreno en el miedo y la complejidad sistémica del problema recién descrito, arraigada en las carencias estructurales de América Latina, donde resulta muchísimo más difícil avizorar formas de sobreponerse a ellas que dejarnos seducir por la utopía de un atajo técnico que nos ofrece aislar al menos una parte del problema y confrontar al monstruo por partes; que nos ofrece, incluso, despolitizar la discusión.

¿Y por qué herejía tecno-optimista? En lo que sigue de estas líneas intentaré explicar por qué la confianza depositada en la capacidad de la tecnología para proveer soluciones útiles y eficientes en el contexto de pandemia contradice los principios y las reglas establecidas de la ciencia, que exige evidencia sólida antes de abrazar la efectividad de una solución o dejar establecida la relación de causalidad entre una acción (intervención tecnológica) y su efecto (mitigación de la pandemia).

Una tipología básica

Luego de semanas de seguir y participar de debates con expertos de múltiples disciplinas, y sin ánimo de resultar exhaustiva, propongo clasificar los distintos roles[2] que se le ha asignado a la tecnología en el en el marco del control de la pandemia, de acuerdo al grado de intrusividad en el ejercicio de los derechos de las personas, ordenadas de menor a mayor:

- Información de salud
- Autodiagnóstico
- Datos integrados para toma de decisiones de salud pública
- Trazabilidad de contactos
- Pasaportes de movilidad y trabajo
- Vigilancia de confinamiento

Cada una de estas esferas cuenta con una gama de posibilidades tecnológicas de implementación, y cada una de ellas ha estado sujeta a diferentes niveles de escrutinio por parte de expertos de diferentes disciplinas. Despiertan también una diversidad de reacciones de la ciudadanía, que las ha visto proliferar en sus distintos contextos locales, y diferentes impactos en el ejercicio de derechos humanos que merecen ser evaluados.

Un repaso crítico a las alternativas tecnológicas disponibles

Información de salud

En lo que se refiere a la disponibilización de información sobre Sars-Cov-2, quien ha marcado el liderazgo ha sido la Organización Mundial de la Salud (OMS) a través de la disponibilización en tiempo real de información científica comprobada —dentro de lo que la corta experiencia de interacción con el virus permite— acerca de los síntomas identificados, procedimientos de tratamiento, protocolos de reducción de exposición al contagio, avances en inmunización y tratamientos paliativos. La OMS ha avanzado en esta labor de cobertura informativa a través de su sitio web, pero también con el reciente lanzamiento de dos aplicaciones[3] y la integración de funcionalidades de chatbot a plataformas de mensajería,[4] con el objetivo de proveer información accesible al público en general, pero también al personal de salud a cargo de lidiar con un virus nuevo, sin entrenamiento específico previo y teniendo que aprender día a día, a expensas de sus propias vidas y las de sus pacientes.

En nuestra región, al esfuerzo de la OMS se alinean los servicios informativos desarrollados a nivel local por varios países a través de páginas web y aplicaciones móviles. Es el caso de Argentina, Bolivia, Chile, Colombia, Perú, Uruguay, entre otros.[5]

En el lado oscuro de esta función informativa de la tecnología están las desastrosas acciones propiciadas por autoridades políticas irresponsables, que promueven el consumo de productos o fármacos de eficacia dudosa, poniendo en riesgo la salud de la población,[6] así como las acciones irreflexivas de personas que, presas del miedo, comparten información falsa que genera más confusión y angustia acerca del origen,[7] los riesgos de contagio,[8] la geopolítica de expansión del virus[9] y los posibles remedios paliativos.[10] Frente a estos villanos de la información en pandemia —o infodemia[11] como se le ha denominado— la otra cara la ofrecen los esfuerzos de verificación de información y de desarrollo de habilidades críticas en el consumo de información por la población desplegados por organizaciones de la sociedad civil[12] e incluso —con mayor o menor éxito— las plataformas privadas[13] que sirven de medio de circulación de la información.

Con todos estos matices, el rol de la tecnología en la facilitación de entrega de información es la funcionalidad de más claro beneficio para los propósitos de control y mitigación de la pandemia, y, por regla general, la capacidad de la tecnología funcionará como amplificadora de la confianza de la que ya gocen o no previamente los emisores de dicha información. No hay tecnología que pueda paliar la falta de confianza en la información científica o en las decisiones políticas que se comunican a través de ella. En tal sentido, la intervención tecnológica será tan fuerte como la legitimidad social de la que gocen los emisores del mensaje, sea la prensa, los organismos internacionales, las empresas de tecnología o los gobiernos nacionales.

Autodiagnóstico

Avanzando un paso más en la complejidad de las respuestas ofrecidas por la tecnología, nos encontramos frente a los servicios web o aplicaciones que se proponen recoger información de síntomas de las personas que los utilizan, con el fin de generar recomendaciones de salud personalizadas en formato de autodiagnóstico.

Las posibilidades aquí pueden abarcar desde la sugerencia de realizar una consulta en servicios de

salud, recomendar una acción de aislamiento social voluntario o simplemente reforzar recomendaciones generales de lavado de manos o distanciamiento social. Se trata de avanzar en la oferta de servicios de telemedicina, de los cuales ya se viene hablando un buen tiempo,[14] pero que ahora se desarrollan bajo la presión de una pandemia en curso.

Aquí es cuando las complejidades de la intervención tecnológica en forma aislada comienzan a hacerse más evidentes. Una herramienta tecnológica de autodiagnóstico es un arma de doble filo: dependiendo de la información que recoge, el modo en que el algoritmo determina el nivel de riesgo y cómo se haya programado el árbol de decisiones que conduce a las distintas recomendaciones, puede generar un número relevante de falsos positivos, es decir, gente que se cree erróneamente enferma y concurre a los servicios de salud, saturándolos. Pero también un cúmulo de falsos negativos, es decir, gente confiada en la capacidad de diagnóstico de la aplicación que no es testeada oportunamente e incurre en situaciones de riesgo de contagio con otros.

Además, el autodiagnóstico solo puede proveer una estrategia exitosa en la mitigación de la pandemia cuando es posible absorber la demanda de atención creada por él. La ausencia de capacidad suficiente de testeo y atención de salud derivada del uso masivo de tecnología de autodiagnóstico puede terminar generando riesgos adicionales de contagios a través de la concurrencia masiva de la población a servicios de salud ya saturados, además de un cuestionamiento en la confianza en el sistema si este se prueba incapaz de responder a la exigencia creada por la tecnología.

Otro riesgo adicional en la calibración de las tecnologías que facilitan el autodiagnóstico es la efectividad de la comunicación que ellas desarrollan: ¿es su lenguaje accesible y claro para todo tipo de personas sin importar su nivel de educación, diversidad lingüística, limitaciones físicas o de alfabetismo digital?

Por último, el diseño de las tecnologías de autodiagnóstico implementadas en la región se ha mostrado altamente intensivo en la recogida de datos personales para generar las recomendaciones personalizadas que entregan, específicamente datos sensibles de salud. La información que se solicita no abarca solamente los síntomas actuales asociados al desarrollo del COVID-19, si no también otra información de condiciones generales y preexistentes de salud, que pone a las usuarias en riesgo de discriminación no solo presente sino también futuro, en términos de acceso a oportunidades de empleo, acceso a seguros de salud y, en general, cualquier actividad que considere la condición de salud como factor de riesgo.

Aún cuando estas aplicaciones y servicios se presentan por las autoridades en la mayor parte de los casos como de uso voluntario, para cumplir su función requieren que se les alimente con información que determine las características físicas, de género y salud de cada usuaria. ¿A dónde van a parar esos datos? ¿Qué condiciones se ofrecen para garantizar su uso exclusivo para diagnóstico de COVID-19? ¿Cómo se garantiza su seguridad y privacidad? Las tecnologías de autodiagnóstico deben evaluarse en este marco integrado, no solo en sus aspectos de impacto en privacidad, si no del ejercicio del derecho de acceso a la salud y de no discriminación en el ejercicio de otros derechos, como los que aquí han sido abordados.

Datos integrados para toma de decisiones de salud pública

En el contexto de pandemia, voces expertas en análisis de datos afirman que 'la luz es el mejor des-

14 Ver https://www.researchgate.net/journal/1530-5627_Telemedicine_and_e-Health

infectante' y, por tanto, exigen que las decisiones de política pública adoptadas para enfrentar la pandemia vayan acompañadas de mayor transparencia de parte de las autoridades en cuanto a la información que las alimenta. En particular, en América Latina —con gobiernos corruptos, incompetentes o con mal expediente de protección de derechos— la sociedad civil exige más información sobre la evolución de la pandemia para poder fiscalizar la toma de decisiones de las autoridades.

De la otra vereda, amparadas en el principio de que mayor cantidad de información contribuye a la mejor calidad de la toma de decisiones, las autoridades también buscan echar mano dentro de sus esquemas normativos (algunos habilitados por la declaración de estados de emergencia y excepción constitucional) y sus posibilidades técnicas para concentrar y cruzar datos públicos previamente en su poder, aunque con otras finalidades, e incluso acceder a datos en manos de las empresas de tecnologías de la información y la comunicación (TICs), para nutrir sus estrategias contra la pandemia.[15] Estas últimas, por supuesto, no han querido restarse y colaborar con la información disponible, para desplegar el poder de los datos para el bien que ya vienen explorando desde antes de la pandemia.[16]

Parece entonces haber relativo consenso respecto a esta necesidad de acceder, cruzar y compartir datos. ¿Qué podría salir mal? La información a la que se busca acceder se refiere a los aspectos más sensibles de la actividad humana: su habitación, sus formas de desplazamiento, hábitos, sus contactos humanos y su condición de salud. El acceso y uso de esa información requiere ser ponderado de acuerdo con el impacto a cada uno de los aspectos de las vidas en juego.

Para avanzar en un abordaje proporcionado en el uso de los datos en el contexto de política pública, debe partirse por abrazar la finalidad de uso de los datos como un principio rector para su recolección. No necesariamente recoger y cruzar más datos es la estrategia más adecuada para conseguir mejores objetivos de política pública. Los datos referidos a personas identificadas o identificables (denominados datos personales) implican riesgos altos no solo de privacidad, si no de discriminación y afectación en el ejercicio de otros derechos humanos en el presente y el futuro.

La anonimización, que se refiere a la desvinculación de una información de la identidad individual de su titular en una forma más o menos irreversible, puede ser un paliativo de los riesgos antes indicados, pero debe ejecutarse adecuadamente y debe ir acompañada de procesos de seguridad operacional, lo que se ha demostrado presenta desafíos técnicos importantes.[17] Por otra parte, los datos agregados o estadísticos pueden presentarse con la suficiente segmentación o categorización para resultar perfectamente útiles a la toma de decisiones de política pública, en relación con la destinación de recursos de salud, capacidad de testeo o decreto de medidas de confinamiento obligatorio, sin poner en riesgo la privacidad y limitando considerablemente los riesgos de afectación de otros derechos.

Soluciones como DAVID-19, propuesta por el Banco Interamericano de Desarrollo en conjunto con la alianza global para el desarrollo del ecosistema de blockchain para América Latina y el Caribe (LACChain)[18] si-

15 Orange, Why is (big) phone data so valuable in combatting the COVID-19 pandemic? 3 de abril de 2020, disponible en: <https://www.orange.com/en/news/2020/April/Why-is-big-phone-data-so-valuable-in-combatting-the-COVID-19-pandemic>

16 Ver https://dataforgood.fb.com/

17 Montjoye, Yves-Alexandre et al. On the privacy-conscientious use of mobile phone data. Scientific Data. 5. 180286. DOI 10.1038/sdata.2018.286, disponible en: <https://www.researchgate.net/scientific-contributions/37748419_Yves-Alexandre_de_Montjoye>

18 Disponible en: https://mellamodavid19.org/

guen esta línea de búsqueda de alternativas tecnológicas que intenten apalancar políticas públicas con el uso de datos. La herramienta, basada en una primera etapa en el aporte voluntario de información de estado de salud y de realización de cuarentena, funciona como una encuesta a través de una página web y una aplicación móvil.

Presentándose como una asistencia a la toma de mejores decisiones de política pública en la región, DAVID-19 pretende "construir, sin exponer datos personales, un mapa regional de cómo la COVID-19 se mueve y evoluciona en tiempo real. La idea es recopilar la información proporcionada para entender quién ha seguido la cuarentena, quién ha mostrado síntomas, y así sucesivamente".

Para los objetivos de política pública hasta aquí analizados, la calidad de los datos recogidos termina siendo un problema fundamental que no resulta fácil de resolver, precisamente por las limitaciones de la tecnología disponible y el contexto social en que las soluciones se insertan. Como abordaremos más adelante, en las consideraciones de contexto local, la calidad de las decisiones de política pública basada en la recogida y cruce de datos depende de la calidad de estos, de su precisión y su representatividad de la población, y esto depende a su vez de las condiciones de acceso a la tecnología, tanto en términos de conectividad como de penetración de la herramienta específica a través de la cual se recogen los datos.

¿Qué datos se recogen con este tipo de tecnologías? Los datos de los conectados, de aquellos que cuentan con dispositivos propios y se encuentran alfabetizados digitalmente, no los datos de la población vulnerable que carece de esos factores. ¿Cuál será entonces la calidad de las políticas pública que descansen sobre esos datos? Esto resulta esencial de ser tenido en consideración para evitar que la toma de decisiones de política pública basadas en los datos recogidos a través de estas tecnologías conduzca a una marginalización adicional de grupos tradicionalmente excluidos, tales como mujeres, niños, adultos mayores, grupos indígenas, comunidades rurales, entre otros.

Una de las categorías de datos más apetitosas que se tocan en este tipo de respuestas tecnológicas es la información de geolocalización (que también juega un rol esencial en otras de las categorías que aquí serán reseñadas) como la trazabilidad de contactos, pasaportes de movilidad y vigilancia del confinamiento. Los datos de geolocalización pueden ser obtenidos a través de información recolectada manualmente o a través de tecnologías de información. Mi dirección en un registro nacional de identidad es información que me geolocaliza en mi residencia habitual, pero la información del GPS de mi teléfono móvil o de las antenas celulares que facilitan su conexión lo hacen en tiempo real donde quiera que vaya.

En contexto de pandemia, la geolocalización de individuos con COVID-19 les expone a riesgos directos de discriminación e incluso de violencia.[19] Sin embargo, la información de geolocalización en forma agregada o anonimizada puede ser no solo útil, si no vital para una mejor toma de decisiones de política pública que determinen acciones de intervención económica y de salud en beneficio de la población, y para una mejor toma de decisiones individuales respecto a lugares u horarios de movilidad menos riesgosa.[20]

Lo importante entonces es comprender para qué es útil esa información y en qué condiciones,[21] ya

19 María José Hermosilla, Violencia y discriminación: ¿Qué gatilla la agresividad que muestran algunas personas en medio de la pandemia? Emol, 23 de abril 2020, disponible en: <https://www.emol.com/noticias/Tendencias/2020/04/23/984027/Discriminacion-Coronavirus-Chile-Contagiados.html>

20 Mana Azarmi & Andy Crawford, Use of Aggregated Location Information and COVID-19: What We've Learned, Cautions about Data Use, and Guidance for Companies, Center for Democracy and Technology, 29 de mayo 2020, disponible en: <https://cdt.org/wp-content/uploads/2020/05/2020-05-29-Use-of-Aggregated-Location-Information-and-Covid-19.pdf>

21 Caroline O. Buckee et al, Aggregated mobility data could help fight COVID-19, Science 145-146, 10 de abril, 2020, disponible en: <https://science.sciencemag.org/content/368/6487/145.2/tab-article-info>

que, como revisaremos en los apartados siguientes, por sus mismas limitaciones técnicas, dicha información presenta más riesgos que beneficios si se pretende utilizar con otros fines, como el de trazabilidad de contactos o vigilancia de confinamiento.

Clave resulta en esta materia que, en el último tiempo, las empresas que proveen servicios móviles han comenzado a desarrollar políticas orientadas a la responsabilidad empresarial por el respeto de los derechos humanos, principios y prácticas que precisamente apuntan a facilitar acceso a la información de geolocalización de sus servicios en una manera compatible al respeto de los derechos fundamentales, al mismo tiempo que sea útil al desarrollo de las políticas públicas. En el contexto COVID-19 se destaca la guía desarrollada a este respecto por la Asociación Internacional de operadores móviles GSMA.[22]

En nuestra región, casos problemáticos de intento de los estados de acceder a los datos en manos de los operadores de telecomunicaciones pueden ser encontrados en Colombia y Brasil. En el caso de Colombia, la Superintendencia de Industria y Comercio expidió la Circular Externa 001 del 23 de marzo de 2020 donde se autoriza a los operadores de telefonía al suministro de información al Departamento Nacional de Planeación y demás entidades estatales que la requieran para "atender, prevenir, tratar o controlar la propagación del COVID-19 (coronavirus) y mitigar sus efectos".[23] La justificación de esta medida a nivel local ha sido la entrega de ayuda económica del Estado frente a la emergencia.[24] Organizaciones de la sociedad civil han rechazado esta circular, señalando que implica riesgos de discriminación, de vigilancia indebida, de invasión de la privacidad y no contempla garantías mínimas frente al tratamiento de dicha información.[25]

En Brasil, la Corte Suprema suspendió una orden del gobierno que exigía a los operadores telefónicos compartir información personal de los clientes con la agencia de estadísticas del país, supuestamente para recopilar datos más completos durante la pandemia. Frente a la medida decretada administrativamente se alzaron voces ante la falta de proporcionalidad y transparencia respecto del uso de la información,[26] lo cual fue confirmado en la decisión de la Corte Suprema que consideró la medida contraria a la protección constitucional de los datos personales, apuntando específicamente a la falta de claridad del propósito de uso de los datos a los que daba acceso la medida y de salvaguardas en su manejo.[27]

Resulta crucial lo que las empresas TICs sean capaces de ofrecer en materia de transparencia sobre la información que se solicita por los gobiernos y se entrega a las autoridades en el contexto de pandemia. De la mano de los Principios Guía de Derechos Humanos y Empresas desarrollados por la ONU en 2011, las

22 GSMA. The GSMA COVID-19 Privacy Guidelines, abril 2020, disponible en: <https://www.gsma.com/publicpolicy/wp-content/uploads/2020/04/The-GSMA-COVID-19-Privacy-Guidelines.pdf>

23 El texto se encuentra disponible en: <https://www.invias.gov.co/index.php/sala/noticias/3763-circular-externa-no-001>

24 Joan López, Ingreso solidario: Un experimento del Estado para evitar discusión política sobre beneficios sociales por COVID 19, Fundación Karisma, 26 de mayo 2020, disponible en: <https://web.karisma.org.co/ingresos-solidario-o-una-barrera-mas-para-la-exigibilidad-de-beneficios-sociales-en-tiempos-de-pandemia/>

25 Organizaciones de la sociedad civil rechazan circular de la SIC sobre uso de datos personales para controlar la pandemia, disponible en: <https://web.karisma.org.co/organizaciones-de-la-sociedad-civil-rechazan-circular-de-la-sic-sobre-uso-de-datos-personales-para-controlar-la-pandemia/>

26 OAB ingressa no STF pela inconstitucionalidade da MP que promove quebra de sigilo de dados telefônicos, AOB, 20 DE ABRIL 2020, disponible en: <https://www.oab.org.br/noticia/58071/oab-ingressa-no-stf-pela-inconstitucionalidade-da-mp-que-promove-quebra-de-sigilo-de-dados-telefonicos>

27 Rafael Zanata y Mariana Marques Rielli., "Please do not share": Brazilian Supreme Federal Court rules in favor of privacy, Access Now, 14 de mayo 2020, disponible en: < https://www.accessnow.org/brazilian-supreme-federal-court-rules-in-favor-of-privacy/>

empresas deben regirse en su actuar por tres ejes: "proteger, respetar y remediar". Para la efectiva vigencia de ese mandato resulta esencial la transparencia corporativa que cubra las acciones de las empresas de TICs, que usan como insumo básico los datos de las personas.

En los últimos años, algunas empresas de TICs han desarrollado la práctica de publicar informes de transparencia, que ha sido una herramienta útil para que los usuarios puedan entender los desafíos y amenazas en la protección de sus derechos. En contexto de pandemia, en el cual proliferan las solicitudes de acceso a datos de los usuarios de algunas de estas empresas, operadores de servicios móviles han comenzado a desarrollar reportes específicos de transparencia.[28] Resulta particularmente interesante saber qué camino tomarán otras empresas de tecnología como Google[29] o Facebook,[30] que a través de sus servicios y aplicaciones, recolectan abundante información de geolocalización, que también está siendo demandada o provista voluntariamente a distintos gobiernos y comunidades científicas.

Si se busca cooperación a través de la entrega de datos agregados por empresas de TICs a los estados, ello debiera realizarse bajo políticas de transparencia en que se les comunique a las usuarias por adelantado qué datos agregados se está considerando entregar a la autoridad, además de abrir canales de diálogo que permitan resolver dudas y cuestionamientos. La información provista al público debe ser suficiente para que se le permita comprender cuál es la utilidad de los datos que se están divulgando, cuáles son los resguardos tomados para proteger la privacidad individual de las usuarias, a quién se entregará acceso a los datos y bajo qué resguardos de seguridad. Existe además una responsabilidad de las empresas de cautelar que los datos sean representativos de todos los segmentos de la sociedad, o que, de no serlos, ello sea explicitado para evitar que sean erróneamente utilizados con fines de toma de decisiones de políticas públicas que conduzcan a la marginalización adicional de la que hemos hablado.

Trazabilidad de contactos

La mayor parte de los análisis y discusiones se han centrado en este limitado segmento de soluciones tecnológicas. A esta altura es posible asumir un cierto grado de familiaridad de la audiencia con el concepto de trazabilidad de contactos, pero vale recordar que esta es una técnica que permite identificar los contactos estrechos de un individuo que ha sido diagnosticado como portador de una enfermedad infectocontagiosa, para poder tomar acciones de salud respecto de tales contactos con el objeto de limitar los riesgos de que continúe la transmisión de la enfermedad. Se trata de un método de larga data de aplicación para la epidemiología, a través de contactos manuales realizados por notificadores humanos, mediante entrevistas presenciales o telefónicas.

Las apps de rastreo de contacto no son más que la tecnologización de la actividad de trazabilidad epidemiológica. Sin embargo, lo que hacen es precisamente separar la actividad de trazabilidad del contacto humano, que siempre ha sido esencial para el éxito de tales estrategias, pues descansan en el conocimiento y

28 Telia Company, freedom of expression and the right to privacy in times of covid-19 – up-dated information on related initiatives and government requests. Up-date june 1st 2020, disponible en: <https://www.teliacompany.com/en/sustainability/responsible-business/freedom-of-expression/#ts-section-74004>

29 Karen Hao, How Facebook and Google are helping the CDC forecast coronavirus, MIT Technology Review, 9 de abril de 2020, disponible en: <https://www.technologyreview.com/2020/04/09/998924/facebook-and-google-share-data-to-forecast-coronavirus/>

30 Ver Covid-19 Mobility Reports, Google, disponible en: <https://www.google.com/covid19/mobility/>

entrenamiento de personal de salud especializado y la posibilidad de entender contextualmente la información que entregan los entrevistados, para medir de forma más precisa su probabilidad de contagio.

Las apps que se crean para generar notificaciones de exposición de contactos potenciales que pueden resultar contagiados de COVID-19 sustituyen ese criterio humano con un algoritmo que define una puntuación de riesgo potencial, en base a variables tales como la distancia del contacto, el tiempo de la exposición, la reiteración del contacto y el tiempo transcurrido entre el diagnóstico y el momento de exposición del contacto; en base a ese riesgo efectuan recomendaciones de acciones de salud para la usuaria, tales como mantenerse en cuarentena preventiva, realizarse un test, concurrir a un servicio de salud, entre otras.

Hasta ahí el modelo parece bastante atractivo, pero si se analiza cada uno de los componentes anteriores es donde comienzan a apreciarse las limitaciones de estas tecnologías. Primero, para que sean realmente efectivas, se requiere una alta adopción por la ciudadanía; estudios científicos específicos indican que entre un 40% y un 60% de la población debe utilizarlas para que tengan impacto relevante en la estrategia sanitaria,[31] aún cuando tasas menores serían útiles en casos de que sean aplicadas en conjunto con otras estrategias tradicionales.[32] Esto de entrada resulta problemático, considerando la disponibilidad de conexión de internet, teléfonos inteligentes y alfabetización digital entre sectores más vulnerables de la población en América Latina y otros países menos desarrollados. ¿Tiene sentido inventir en un despliegue de esta tecnología para cubrir solo a los sectores más privilegiados de la sociedad e invisibilizar a través de los datos recolectados a los marginados de siempre?

Segundo, la tecnología que ha adquirido mayor aceptación hasta el momento para el desarrollo de estas apps es la de Bluetooth,[33]-básicamente porque tanto el GPS[34] como la información de las antenas celulares carece de precisión para medir contactos de menos de dos metros, que es la distancia relevante para la transmisión de COVID-19.[35] Específicamente, el protocolo Bluetooth de baja energía (BLE) es el que ha sido considerado para el desarrollo de las soluciones de trazabilidad de contactos por su precisión y ahorro de energía, pero se debe tener en consideración que, a pesar de haber sido desarrollado desde 2010, la versión 5.0 que cuenta con mayor alcance de señal solo se encuentra presente en los teléfonos inteligentes más modernos, fabricados desde 2017 en adelante.[36]

Además, la tecnología Bluetooth no está exenta de imprecisiones.[37] Basta activarlo en tu teléfono

31 Luca Ferretti, Chris Wymant, Michelle Kendall, Lele Zhao, Anel Nurtay, Lucie Abeler-Dörner, Michael Parker, David Bonsall, Christophe Fraser, Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing, Science08, Mayo 2020, disponible en: <https://science.sciencemag.org/content/early/2020/03/30/science.abb6936/tab-pdf>

32 Patrick Howell O'Neill, No, coronavirus apps don't need 60% adoption to be effective, MIT Technology Review, 5 de junio 2020, disponible en: <https://www.technologyreview.com/2020/06/05/1002775/covid-apps-effective-at-less-than-60-percent-download/>

33 Ver Privacy International, Bluetooth tracking and COVID-19: A tech primer, 31 de marzo 2020, disponible en: <https://www.privacyinternational.org/explainer/3536/bluetooth-tracking-and-covid-19-tech-primer>

34 National Coordination Office for Space-Based Positioning, Navigation, and Timing, Official U.S. government information about the Global Positioning System (GPS) and related topics, GPS Accuracy, 22 de abril 2020, disponible en: <https://www.gps.gov/systems/gps/performance/accuracy/>

35 Jay Stanley & Jennifer Stisa Granick, The Limits of Location Tracking in an Epidemic, ACLU, 8 de abril, 2020, disponible en: <https://www.aclu.org/sites/default/files/field_document/limits_of_location_tracking_in_an_epidemic.pdf>

36 Alberto García, No todos los móviles tienen el mismo Bluetooth 5: cómo diferenciarlo, ADSLZone, 1 de abril 2020, disponible en: <https://www.adslzone.net/2019/04/01/bluetooth-5-funciones-opcionales-diferencias/>

37 Douglas J. Leith & Stephen Farrell, Coronavirus Contact Tracing: Evaluating ThePotential Of Using Bluetooth Received Signal Strength For Proximity Detection, School of Computer Science & Statistics, Trinity College Dublin, Ireland, 6 de Mayo 2020, disponible en: <https://www.scss.tcd.ie/

para que puedas detectar el móvil o los parlantes de tu vecino, aunque los separe un muro y no se hayan cruzado en lo que va de cuarentena. Entonces, aún esta tecnología arroja múltiples falsos positivos, que podrían terminar atochando los servicios de salud, así como múltiples falsos negativos, que pueden generar un efecto placebo que resulte en un impacto perjudicial en la población, que confiando en el uso de la app terminen relajando otras medidas más esenciales, como el distanciamiento social o el lavado de manos.

Tercero, para el funcionamiento de estas apps es posible —aunque no necesario— recolectar una gran cantidad de información de sus usuarias, lo cual depende de su diseño y del compromiso con el respeto a la privacidad, y de su uso exclusivo con la finalidad de mitigación de la pandemia. Aquí es donde el tema se enreda considerablemente y ha sido pobremente manejado por quienes han estado promoviendo el uso de estas tecnologías en muchos países. El objetivo de estas apps debe limitarse a la identificación de posibilidades de contacto entre personas en riesgos de transmisión de COVID-19. Para eso no se necesita conocer la identidad de las personas ni su ublicación.

La OMS desarrolló un trabajo en esta materia con un comité multidisciplinario de expertos, con los cuales elaboró una guía de principios éticos, consideraciones técnicas y requisitos que son consistentes con estos principios para lograr el uso equitativo y apropiado de estas tecnologías con el propósito de informar a los programas de salud pública y a los gobiernos que están considerando desarrollar o implementar tecnologías digitales de trazabilidad para el seguimiento de contactos COVID-19.[38]

Tales principios resultan útiles y orientadores para la toma de decisiones y fueron elaborados teniendo a la vista las diferentes alternativas técnicas disponibles hasta ahora, de acuerdo a los distintos proyectos técnicos que, contra reloj, se han desarrollado alrededor del mundo para responder a los desafíos de la pandemia. Pasemos a examinar brevemente esas diferentes alternativas técnicas desde una perspectiva crítica.

Como hemos visto ya, además de su mayor granularidad comparado con las tecnologías de GPS y antenas móviles, los protocolos desarrollados sobre la base de la tecnología BLE —como los utilizados en Singapur, Australia, la interfaz desarrollada por Apple/Google y varios de los propuestos en Europa— consiguen con mayor claridad objetivos de protección de la privacidad pues no recolectan información de localización, ni la identidad de las personas que usan la app que los conecta a las usuarias. Lo que hacen es permitir recolectar identificadores que se crean en forma aleatoria y se almacenan temporal y localmente en los dispositivos, y solo se comunican a la autoridad de salud (en los sistemas centralizados) o a los demás usuarios (en los sistemas descentralizados) cuando una usuaria recibe un diagnóstico positivo.

Los elementos esenciales de estos sistemas son: (i) dispsitivos en poder de las usuarias que generan y almanencan identificadores aleatorios efímeros; (ii) un operador de servicios back-end que permite la comunicación entre dispositivos y la confirmación de casos de infección a través de comunicaciones cifradas (en el casos de los modelos centralizados una autoridad juega este rol y provee más que solo back-end, adicionando almacenamiento y filtrado de información); y, (iii) una app que permite la comunicación con las usuarias. Usualmente se concibe que sea una autoridad quien esté a cargo de este componente, de modo de hacer que este se incerte en las capacidades de respuesta de la pandemia, permita la calibración del riesgo computado

---

Doug.Leith/pubs/bluetooth_rssi_study.pdf>

38 World Health Organization, Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing, 28 de mayo 2020, disponible en: <https://apps.who.int/iris/bitstream/handle/10665/332200/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1-eng.pdf>

y de las recomendaciones de salud realizadas conforme a este.

Revisemos brevemente las variantes de protocolos de trazabilidad de contactos o notificaciones de exposición basadas en el uso de BLE que han sido propuestas, con un énfasis particular en el debate de los beneficios y riesgos de las soluciones descentralizadas, centralizadas o mixtas, así como la discusión creciente acerca de la interoperabilidad como condición esencial de su éxito y contribución a la mitigación de la pandemia.

Sin ánimo exhaustivo, a la fecha los principales protocolos descentralizados que han adquirido notoriedad en la búsqueda de sistemas de notificación de exposición son: DP3T,[39] desarrollado por un consorcio de académicos europeos; PACT,[40] desarrollado por un consorcio de académicos de los Estados Unidos; la interfaz de aplicación (API) desarrollada en forma conjunta por Apple y Google,[41] desarrollada como un esfuerzo de interoperabilidad de las gigantes tecnológicas; y TCN Protocol,[42] también desarrollada en los Estados Unidos por una coalición de expertos en seguridad. Los componentes básicos de todas estas soluciones son los mismos ya descritos y todas operan de forma descentralizada, es decir que el almacenamiento de los identificadores efímeros se produce a nivel local en los dispositivos y, en caso de diagnóstico de infección, los identificadores del infectado son transmitidos para que los dispositivos de quienes hayan estado expuestos a un contacto con el dispositivo del paciente diagnosticado puedan reconocerlo y, conforme al riesgo computado, generar una notificación a su titular.

Las ventajas principales de estos sistemas descentralizados son la minimización de información recolectada (exclusivamente los identificadores efímeros, pero no localización, ni otra información que permita identificar a las usuarias) lo que previene abusos de la autoridad a través del usos de datos para fines distintos de los de salud; almacenamiento localizado y temporal en el dispositivo por alrededor de 15 días, de acuerdo a la relevancia epidemiológica determinada hasta hoy, con lo cual se previene la posibilidad de monitoreo malicioso de personas infectadas; y que el sistema asegura su desmantelamiento automático pues no existen datos almacenados centralmente, con lo cual, si deja de haber infectados, dejará de existir información disponible que alimente al sistema. Sobre este último punto, resulta necesario llamar la atención a que, de acuerdo con lo informado por las empresas, la API ofrecida por Apple/Google permite una deshabilitación regional de su funcionalidad por diseño.

Todas las soluciones descentralizadas requieren de una interfaz a las usuarias a través de una app que se comunique con ellas. En el caso de la solución provista por Apple/Google, las empresas han optado por no hacerse cargo de esta componente del sistema, dejando a las autoridades locales la responsabilidad de tales desarrollos. Esta opción abre la puerta a que las implementaciones de gobiernos locales puedan incorporar en sus apps otros requerimientos de recogida de información que excedan el diseño y las características de preservación de la privacidad presentado por el modelo hasta aquí explicado.

Aun cuando Apple/Google presentan términos y condiciones de uso de su API[43] que pretenden blin-

39 Carmela Troncoso et al. Decentralized Privacy Preserving Proximity Tracing. 25 de mayo 2020, disponible en: <https://arxiv.org/ftp/arxiv/papers/2005/2005.12273.pdf>

40 Justin Chan et al. PACT: Privacy-Sensitive Protocols And Mechanisms for Mobile Contact Tracing, 7 de mayo 2020, disponible en: <https://arxiv.org/pdf/2004.03544.pdf>

41 Apple & Google, Privacy-Preserving Contact Tracing, abril 2020, disponible en: <https://www.apple.com/covid19/contacttracing/>

42 TCN coalition, TCN Protocol, abril 2020, disponible en: <https://github.com/TCNCoalition/TCN>

43 Ver GoogleCOVID-19ExposureNoticationsServiceAdditionalTerms, 4 de mayo 2020, disponible en: <https://blog.google/documents/72/Expo-

dar el uso de esta tecnología de formas no alineadas con la protección de la privacidad —particularmente, exigen uso voluntario, no utilización para otros propósitos, prohíben un uso discriminatorio, establecen una imposibilidad técnica de acceder a la localización de los dispositivos y de acceder automáticamente a agenda de contactos—, restará ver cuál será la adhesión efectiva de las autoridades locales a tales condiciones, así como cuál será la conducta de las empresas para asegurar el respeto por tales condiciones cuando comiencen a desplegarse la implementación de aplicaciones bajo esta tecnología.[44]

Entre los protocolos centralizados que se han desplegado a la fecha, el de mayor notoriedad es BlueTrace[45] adoptado por Australia (CovidSafe) y Singapur (TraceTogether), basado también en la recogida de señales BLE, pero con registro y almacenamiento centralizado por la autoridad de salud de los identificadores asociados a un número de teléfono. Un elemento interesante de los modelos centralizados como este es que permiten combinar la información de la app con aquella obtenida de las entrevistas desarrolladas a través de la identificación manual de contactos.

El protocolo funciona de la siguiente manera: las usuarias transmiten identificaciones de aspecto aleatorio y recopilan identificaciones en su proximidad. Luego, al recibir un diagnóstico positivo, la usuaria informa a la autoridad todas las identificaciones recopiladas en su proximidad durante la ventana de infección pertinente. La autoridad entonces alerta a las usuarias que generaron estas identificaciones. Se utiliza un sistema de cifrado simétrico para las identificaciones temporales, cuya llave se encuentra exclusivamente en poder de la autoridad. La usuaria puede revocar en cualquier momento su consentimiento, eliminando su número del registro y, con ello, la posibilidad de asociar los identificadores efímeros generados a su identidad.

Open Trace es la versión código abierto de la aplicación TraceTogether, originalmente lanzada por Singapur, y que fue una de las primeras en desplegarse y encender el debate acerca del uso de aplicaciones móviles para la trazabilidad de contactos. Polonia está entre los países que han implementado este protocolo a través de su ProteGO Safe app.[46] Un estudio técnico reciente muestra que la aplicación funciona utilizando los servicios Firebase Analytics provistos por Google, lo que posibilita que dicha empresa tenga acceso a la información individualizada de los usuarios, aunque solo sea compartida en forma agregada a la autoridad.[47]

ROBERT es otro protocolo centralizado en base a BLE desarrollado en Francia, bajo la premisa de que, además de tratarse de una solución tecnológica que preserve la privacidad, debe tratarse de una que permita controlar las posibilidades de ataques externos al sistema, que disminuyan su estabilidad y la confianza en este. Se presentó como una alternativa crítica de los inconvenientes de seguridad por ataques externos, principal debilidad de los sistemas descentralizados antes examinados, ya que pueden generarse artificialmente e inyectarse al sistema identificaciones efímeras con la finalidad de hacer que un grupo específico de

---

sure_Notifications_Service_Additional_Terms.pdf>

44 Al momento de escribir este documento Alemania, Austria, Italia, Grecia, Portugal y Suiza se encontraban evaluando posibilidades de implementación. En América Latina se ha hecho mención de de Uruguay como potencial lugar de implementación.

45 Jason Bay, Joel Kek, Alvin Tan, Chai Sheng Hau, Lai Yongquan, Janice Tan, Tang Anh Quy, BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders, Government Technology Agency of Singapore, 9 de abril 2020, disponible en: <https://bluetrace.io/>

46 Malgorzata Fraser, Coronavirus contact tracing reignites Polish privacy debate, DW, 30 de mayo 2020, disponible en: <https://www.dw.com/en/coronavirus-contact-tracing-reignites-polish-privacy-debate/a-53600913>

47 Douglas J. Leith & Stephen Farrell, Coronavirus Contact Tracing App Privacy: WhatData Is Shared By The Singapore OpenTrace App?, School of Computer Science & Statistics,Trinity College Dublin, Ireland, 28 de abril 2020, disponible en: <https://www.scss.tcd.ie/Doug.Leith/pubs/opentrace_privacy.pdf>

individuos parezca en riesgo de exposición y sea masivamente notificado (denominado riesgo de "ataque terrorista").[48] El protocolo se basa en un esquema que combina una infraestructura de servidor federado e identificadores anónimos temporales, con el control y administración de los puntajes de riesgo y las notificaciones por el servidor de la autoridad de salud, lo que conforme a sus autores proporciona alta robustez, flexibilidad y eficacia.[49]

Presentado como una evolución de ROBERT, el protocolo mixto DESIRE,[50] desarrollado en colaboración por académicos franceses y alemanes, descentraliza la mayoría de las operaciones necesaria en el sistema de notificación de exposición. La principal diferencia con ROBERT es que se crean tokens de encuentro privado (PET) secretos y generados criptográficamente, para codificar encuentros. La función del servidor es simplemente hacer coincidir los PET generados por los usuarios diagnosticados con los PET proporcionados por los usuarios solicitantes, información que se almacena cifrada en el servidor, pero controlada por llaves almacenadas en los dispositivos (criptografía asimétrica). Esta mejora se plantea con la finalidad de generar una mejor protección contra usuarios y autoridad maliciosos. Sin embargo, como en ROBERT, los puntajes de riesgo y las notificaciones aún son administradas y controladas por el servidor bajo control de la autoridad de salud.

Por último, aunque no se trata de protocolos técnicos en sí, si no de la combinación de uso de distintas tecnologías y fuentes de información, vale la pena destacar el caso de las soluciones desarrolladas en India, Corea del Sur y Nueva Zelandia. Aarogya Setu es la app implementada en forma obligatoria para acceder a los lugares de trabajo en India. La app utiliza señales de Bluetooth para registrar contactos en la forma antes descrita, pero además utiliza datos de ubicación GPS para aumentar la información recopilada y construir una base de datos centralizada de la propagación de la infección, un enfoque que la mayoría de los países evita por razones de privacidad. También imita el sistema de código QR de salud de China —que examinaremos luego— con una función que califica el estado de salud probable de una persona con colores verde, naranja o rojo para indicar si una persona está segura, en alto riesgo o es portadora del virus. Por disposición administrativas del Ministerio de Tecnología de India, la agencia gubernamental que desarrolló la app es libre de compartir datos personales de la aplicación con otras agencias gubernamentales e instituciones de salud pública.[51]

En Corea del Sur se ha implementado una app que usa la información de antenas de telefonía móvil para el rastreo de contactos y potenciar la trazabilidad tradicional a través de entrevistas. La autoridad combina datos de ubicación de teléfonos móviles, registros de transacciones de tarjetas de crédito y grabaciones de circuito cerrado de televisión para rastrear y evaluar a las personas que podrían haber entrado recientemente en contacto con una persona infectada. Lo anterior ha ido acompañado de la publicación de mapas

48 Ver Ross Anderson, Contact Tracing in the Real World, 12 de abril 2020, Light Blue Touchpaper, disponible en: <https://www.lightbluetouchpaper.org/2020/04/12/contact-tracing-in-the-real-world/>

49 PRIVATICS team, ROBERT: ROBust and privacy-presERving proximity Tracing, 19 de abril, 2020, disponible en: <https://github.com/ROBERT-proximity-tracing/documents/blob/master/ROBERT-specification-EN-v1_0.pdf>

50 Claude Castelluccia, Nataliia Bielova, Antoine Boutet, Mathieu Cunche, Cédric Lauradoux, et al. DESIRE: A Third Way for a European Exposure Notification System Leveraging the best of centralizedand decentralized systems, 12 de mayo 2020, disponible en: <https://hal.inria.fr/hal-02570382/file/DESIRE-specification-EN-v1_0.pdf>

51 Sankalp Phartiyal, India follows China's lead to widen use of coronavirus tracing app, Reuters, 14 de mayo 2020, disponible en: <https://www.reuters.com/article/us-health-coronavirus-india-app/india-follows-chinas-lead-to-widen-use-of-coronavirus-tracing-app-idUSKBN22Q110>

detallados que muestran movimientos precisos de personas infectadas, alentando a otros que podrían haber estado en contacto con ellos a realizarse exámenes, pero también ocasionando graves consecuencias sociales por el riesgo de re-identificación de las personas contagiadas.[52]

Nueva Zelandia ha adoptado una aproximación interesante basada en el principio de amplificar la capacidad de trazadores humanos trabajando para el sistema de salud. Para ello, mezcla elementos de la tecnología QR implementada en China, pero sin que la información se almacene centralizadamente, si no en forma local en los dispositivos de las usuarias, como un registro de cada uno de los establecimientos que la usuaria visita en los cuales deberá escanear el código QR. En caso de determinarse una infección, la información de lugares visitados será requerida por personal de salud para hacer el cruce con el registro de usuarias disponible en los establecimientos que aparezcan en el registro. Notablemente, el gobierno neozelandés acompañó el lanzamiento de su app de una evaluación de impacto en privacidad y anuncia que este será un proceso constante durante le despliegue de dicha tecnología.[53]

Como puede concluirse de esta muy apretada revisión, todas las alternativas técnicas disponibles cuentan con riesgos en su operación necesarios de calibrar a la hora de desarrollar su implementación, y aunque las soluciones descentralizadas han ido acompañadas de un mayor consenso técnico por su características de preservación de privacidad y limitación de posibilidad de desvío de uso de la autoridad, ellas no son inmunes a riesgos de seguridad si se trata de analizar ataques de mayor sofisticación. Así también, su eficiencia dependerá de la configuración del algoritmo encargado de determinar el riesgo de infección, que sigue encontrándose en todos los casos en manos de una autoridad de salud competente.

Finalmente, la interoperabilidad de soluciones es un componente que se ha levantado como esencial de cara al progresivo levantamiento de medidas restrictivas de cruce de fronteras y a la proliferación de distintas soluciones tecnológicas, incluso dentro de un mismo país o región. En Europa, los estados parte de la eHealth Nework han relevado la necesidad de interoperabilidad dentro de la región,[54] y un grupo de expertos trabajando en diferentes protocolos descentralizados han comenzado a explorar las alternativas técnicas para alcanzar dicha interoperabilidad.[55] Discusiones de soberanía tecnológica se mezclan en la combinación de las diferentes soluciones propuestas, incluyendo la conveniencia de descasar en la tecnología provista por los gigantes Americanos Apple/Google, y la proliferación de protocolos, tanto para soluciones centralizadas como descentralizadas y mixtas agrega complejidad adicional a la posibilidad de alcanzar la interoperabilidad.

Sin embargo, coincidimos en que la interoperabilidad será la prueba final de eficacia que esta tecnología de trazabilidad de contactos deberá enfrentar de cara a un mundo que intente reactivarse y alcanzar su tan ansiada nueva normalidad.

52 BBC, Coronavirus privacy: Are South Korea's alerts too revealing?, BBC News, 5 de marzo 2020, disponible en: <https://www.bbc.com/news/world-asia-51733145>

53 Ministry of Health of New Zeland, COVID-19 Contact Tracing Application, Privacy Impact Assessment, 15 de mayo 2020, disponible en: <https://www.health.govt.nz/system/files/documents/pages/nz_covid_tracer_pia_18_may_2020.pdf>

54 eHealth Network, Interoperability guidelines for approved contact tracing mobile applications in the EU, 13 de mayo 2020, disponible en: <https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf>

55 Ulrich Luckas et al. Interoperability of decentralized proximity tracing systems across regions, 15 de mayo 2020, disponible en: <https://drive.google.com/file/d/1mGfE7rMKNmc51TG4ceE9PHEggN8rHOXk/edit>

Pasaportes de movilidad y trabajo

Los pasaportes de inmunidad buscan generar un grado de certeza que permita la circulación de la población y la reactivación de las actividades económicas y sociales. Su emisión depende de la existencia de métodos de medición de los grados de inmunidad desarrollada por la población frente a una enfermedad infectocontagiosa. Su objetivo es precisamente discriminar entre aquellos que cuentan con inmunidad y quienes carecen de ella, asignando consecuencias de movilidad y oportunidades de empleo a esa clasificación. Así, buscan imponer una restricción artificial sobre quién puede participar en actividades sociales y económicas, y quién no.

Es por ello que los expertos llaman la atención acerca del riesgo de que los pasaportes de inmunidad creen un incentivo perverso para que las personas busquen infectarse, especialmente las más vulnerables, que no pueden permitirse un período de exclusión de la fuerza laboral, agravando las desigualdades sociales preexistentes.[56] Las situaciones de corrupción o debilidad institucional en América Latina y otros países menos desarrollados pueden ocasionar que este tipo de herramientas profundicen el daño en el ejercicio de derechos económicos y sociales sufrido a causa de la COVID-19 por las poblaciones más vulnerables.

China fue el primer país en implementar este tipo de herramientas en el contexto de la pandemia, a través de un sistema codificado de colores tipo semáforo, asociado a un código QR que se vincula a la identidad de cada persona y permite regular la movilidad en espacios públicos. Contar con un código verde es exigido para habilitar el viaje entre provincias, y los establecimientos y servicios de atención a público pueden condicionar el acceso a las personas a contar con un código verde. No existe transparencia respecto de los factores de riesgo y la ponderación que determina la asignación de los colores. Además de almacenar información de movilidad, la aplicación registra información de salud declarada por el paciente y su ficha médica. La herramienta además se encuentra integrada a plataformas preexistentes de amplia adopción en ese país, como son la plataforma de pago Alipay y la de mensajería WeChat.[57] En los últimos días, algunos gobiernos locales anunciaron la intención de hacer el sistema permanente para monitorear la salud de su población dentro de su ciudad.[58]

Recientemente, añadiendo a las tecnologías previamente desplegadas por Corea del Sur desde el inicio de la pandemia para mantener el monitoreo de pacientes de COVID-19, la autoridad de control de enfermedades y desastres anunció que planea introducir un sistema de registro electrónico a través de códigos QR para controlar la entrada en instalaciones consideradas de alto riesgo de propagación de SARS-CoV-2, incluidos los recintos de entretenimiento. La sociedad civil de ese país ha manifestado preocupación de que el gobierno esté tratando de establecer un sistema de vigilancia y control más completo en nombre de la prevención de la epidemia.[59]

56 Alexandra L Phelan, COVID-19 immunity passports and vaccination certificates: scientific, equitable, and legal challenges, The Lancet Vol 395, 23 de mayo, 2020, disponible en: <https://www.thelancet.com/action/showPdf?pii=S0140-6736%2820%2931034-5>

57 Helen Davidson, China's coronavirus health code apps raise concerns over privacy, The Guardian, 1 de abril 2020, disponible en: <https://www.theguardian.com/world/2020/apr/01/chinas-coronavirus-health-code-apps-raise-concerns-over-privacy>

58 Helen Davidson, Chinese city plans to turn coronavirus app into permanent health tracker, The Guardian, 26 de mayo, disponible en: <https://www.theguardian.com/world/2020/may/26/chinese-city-plans-to-turn-coronavirus-app-into-permanent-health-tracker>

59 Miru Lee, In the era of COVID-19, is S.Korea's 'new normal' a digital surveillance state? Jinbo Net, 26 e mayo 2020, disponible en: <http://act.jinbo.net/wp/43070/>

En el Reino Unido se han anunciado iniciativas público-privadas para desarrollar pasaportes epidemiológicos basados en tecnología de reconocimiento facial.[60] La app desarrollada por el servicio de salud del Reino Unido ya permite su activación a través de reconocimiento facial, para lo cual requiere que los usuarios envíen una fotografía de sí mismos de un documento oficial, como su pasaporte o licencia de conducir, con lo cual se está preparando la base de datos que podría ser utilizada para los pasaportes de inmunidad.[61]

La OMS ha expresado su preocupación por el desarrollo de pasaportes de inmunidad, advirtiendo la información insuficiente acerca del desarrollo de anticuerpos para el SARS-CoV-2, con los riesgos de errónea clasificación de los niveles de inmunidad de la población que ello podría implicar. A través de este tipo de certificaciones, puede terminar comunicándose un erróneo mensaje acerca de la inmunidad con que contaría la población en el evento de una segunda oleada de infección, generándose el riesgo de que la población ignore los consejos de salud pública más generales y, con ello, incremente los riesgos de transmisión continua.[62]

En América Latina, Chile había anunciado con bastante fanfarria la preparación de un carnet de inmunidad digital, sin embargo, la iniciativa fue suspendida frente a los cuestionamientos surgidos desde la OMS.[63]

El nivel de incertidumbre científica acerca del desarrollo de inmunidad respecto del SARS-CoV-2, así como las devastadoras consecuencias económicas y sociales que podría tener la implementación de este tipo de iniciativas, llaman a la extrema cautela en su evaluación, la que de ser implementadas con posterioridad solo podrían resultar necesarias y proporcionadas si se desarrollan acompañadas de un marco regulatorio que prevenga su uso con fines discriminatorios incompatibles con el ejercicio de derechos humanos. Existe vasta experiencia previa desde la normativa de protección de los derechos de los trabajadores acerca de los riesgos de permitir decisiones de empleo atendidas a condiciones de salud, y esa experiencia será sin duda útil para calibrar los derechos en juego. Estos pasaportes no deberían resultar en una herramienta de control social que restrinja la movilidad de la población en contextos de disidencia política o una herramienta adicional para imponer restricciones abusivas a la migración, por nombrar solo algunos de los potenciales impactos negativos de estas implementaciones.

Vigilancia de confinamiento

El brazalete electrónico como fórmula de control de cumplimiento de medidas de confinamiento está siendo utilizado en Bulgaria, Corea del Sur y Hong Kong.[64] En Corea del Sur la medida parece tener carácter punitivo, al ordenarse en caso de detecciones de incumplimiento previo de órdenes de confina-

60 Kate Proctor and Hannah Devlin, Coronavirus UK: health passports 'possible in months', The Guardian, 4 de mayo 2020, disponible en: <https://www.theguardian.com/politics/2020/may/03/coronavirus-health-passports-for-uk-possible-in-months>

61 Jane Wakefield, Coronavirus: NHS app paves the way for 'immunity passports', BBC, 27 de mayo 2020, disponible en: < https://www.bbc.com/news/technology-52807414>

62 Immunity passports" in the context of COVID-19, 24 de abril 2020, disponible en: <https://www.who.int/news-room/commentaries/detail/immunity-passports-in-the-context-of-covid-19>

63 Christian Leal, Gobierno posterga por posible "discriminación odiosa" entrega de polémico carnet Covid-19, Biobio, 10 de mayo 2020, disponible en: <https://www.biobiochile.cl/noticias/nacional/chile/2020/05/10/gobierno-posterga-por-posible-discriminacion-odiosa-entrega-de-polemico-carnet-covid-19.shtml>

64 BBC News, Coronavirus: People-tracking wristbands tested to enforce lockdown, 24 de abril 2020, disponible en: <https://www.bbc.com/news/technology-52409893>

miento, situación en la cual el infractor puede escoger el uso del brazalete como una alternativa para no ser llevado a una residencia sanitaria en que se vigile el cumplimiento de su cuarentena.[65]

En Polonia se exige que las personas en cuarentena descarguen una aplicación y la usen para cumplir con las indicaciones recurrentes de tomarse una selfie con un sello de tiempo y lugar, y luego enviar la foto al gobierno. El incumplimiento de esta exigencia puede resultar en intervención policial en el domicilio de los contagiados y una multa. Los datos recogidos por la app se conservan durante seis años y la policía, los gobernadores, el Centro de Tecnología de la Información, el Centro Nacional de Sistemas de Información de Salud y el subcontratista que desarrolla la aplicación puede acceder a ellos.[66]

En Israel, tecnología previamente desplegada por servicios de inteligencia contra el terrorismo intentó ser reacomodada al propósito de vigilancia de cuarentena, en el marco de la declaración de Estado de Emergencia[67] y, mientras estuvo vigente, ocasionó el arresto de más de 200 personas,[68] antes de ser declarada ilegal por la Corte Suprema. Adicionalmente, drones se usan para patrullar y verificar el cumplimiento de cuarentenas,[69] similar a lo que estaría sucediendo en Paraguay, a través de la donación por privados al Ministerio del Interior de uno de esos dispositivos.[70]

En Taiwán, se adoptó en febrero un sistema de 'cerca digital', mediante el cual la ubicación de cualquier persona que deba someterse a la cuarentena obligatoria se controla a través de la señal celular de su teléfono. La medida se ha implementado en el contexto de la normativa específica existente en ese país para el control de enfermedades y el gobierno se ha comprometido a desmantelar el sistema una vez terminada la emergencia, y no utilizar sus datos para investigaciones criminales.[71]

Algo similar fue anunciado en Ecuador como parte del Decreto a través del cual se declaró estado de emergencia, en el cual se señaló que "[p]ara el cumplimiento de las restricciones del presente Decreto se podrán utilizar plataformas satelitales y de telefonía móvil para monitorear la ubicación de personas en estado de cuarentena sanitaria y/o aislamiento obligatorio, que incumplan las restricciones dispuestas, a fin de ponerlas a disposición de las autoridades judiciales y administrativas competentes". La sociedad civil de la región reaccionó con preocupación a este anunciando, señalando que esta medida reviste particular gravedad en un contexto en que, a pesar de la garantía de la privacidad consagrada en el artículo 66 numerales 11, 19 y 20 de la Constitución de la República, Ecuador carece a la fecha de una normativa legal y de una autoridad

65 Park Han-na, Tracking wristband launched to deter quarantine breakers, The Korea Herald, disponible en: < http://www.koreaherald.com/view.php?ud=20200427000967>

66 Katri Uibu, Poland is making its citizens use a 'selfie' app during the coronavirus crisis, 24 de abril 2020, disponible en: <https://www.abc.net.au/news/2020-04-25/coronavirus-poland-tracking-quarantine-selfie-app/12173884>

67 BBC News, Coronavirus: Israel halts police phone tracking over privacy concerns, 23 de abril 2020, disponible en: <https://www.bbc.com/news/technology-52395886>

68 Maayan Lubell, Israel's top court says government must legislate COVID-19 phone-tracking, Reuters, 26 de abril 2020, disponible en: <https://www.reuters.com/article/us-health-coronavirus-israel-monitoring/israels-top-court-says-government-must-legislate-covid-19-phone-tracking-idUSKCN2280RN>

69 Joseph Krauss, Israeli police use drones to enforce virus quarantines, raising privacy concerns, The times of Israel, 14 de abri, 2020, disponible en: <https://www.timesofisrael.com/israeli-police-using-drones-to-enforce-coronavirus-quarantines/>

70 Paloma Lara, Uso de drones: ¿combaten la pandemia o refuerzan el control ciudadano?, TEDIC, 20 de abril 2020, disponible en: <https://www.tedic.org/uso-de-drones-covid19/>

71 Arthur Shay, Cell site location information helps digital fencing against COVID-19 pandemic, ILO, 24 de abril 2020, disponible en: <https://www.internationallawoffice.com/Newsletters/Tech-Data-Telecoms-Media/Taiwan/Shay-Partners/Cell-site-location-information-helps-digital-fencing-against-COVID-19-pandemic>

técnica e independiente que permita una adecuada supervisión de que las medidas a implementarse respeten los principios de adecuación, necesidad y proporcionalidad compatibles con el estado de derecho.[72]

El uso de tecnologías de vigilancia para fiscalizar el confinamiento presenta un claro cuestionamiento de proporcionalidad en la fuerza por parte del Estado. Medidas que restringen la libertad en función de una condición de salud no pueden significar una oportunidad de restricción para las libertades públicas y derechos de las personas afectadas, que no son responsables de delito alguno.

La normalización de esos niveles de vigilancia individual en función de la salud pública constituye un precedente de limitación de libertades que fácilmente puede ser reposicionado en el futuro para los más diversos fines por las fuerzas políticas dominantes, cuestión que siempre terminará por acarrear un riesgo desproporcionado de afectación a minorías y grupos vulnerables, y la amenaza de sustituir las democracias por un autoritarismo sin contrapesos.

72 Derechos Digitales, Ecuador: Las tecnologías de vigilancia en contexto de pandemia no deben poner en riesgo los derechos humanos, 18 de marzo 2020, disponible en: <https://www.derechosdigitales.org/14285/ecuador-las-tecnologias-de-vigilancia-en-contexto-de-pandemia-no-deben-poner-en-riesgo-los-derechos-humanos/>

Una App para gobernarlos a todos

Una estrategia marcada en las diferentes iniciativas gubernamentales de implementaciones tecnológicas que han florecido en la región —y en el mundo— ha sido la de combinar en una app distintas funciones de las identificadas en la tipología propuesta. No son pocas las aplicaciones que van desde la entrega de información general sobre medidas a los cuestionarios o chatbots que permiten interacción para el autodiagnóstico, y que a la vez recogen información de geolocalización a través de la solicitud de activación de GPS, la que puede después ser usada en forma agregada para decisiones de política pública, mientras las más osadas pretenden cautelar el cumplimiento de cuarentenas.

Esta aproximación de empaquetamiento hace difícil identificar con claridad los riesgos y beneficios que traen aparejadas las tecnologías con las que se pretende seducir. También hace aún más problemático el rol del consentimiento en términos de tener la posibilidad de escoger entre las funcionalidades ofrecidas aquellas que sean menos problemáticas. Tal como sucede en el ámbito de la competencia y protección de los derechos del consumidor, estos empaquetamientos debieran encontrarse limitados, ya que erosionan la agencia de las personas en una materia tan relevante como su información de salud.

La última cuestión preocupante en este sentido es el riesgo de que esta fórmula de empaquetamiento alcance a los beneficios económicos que se distribuyen a los sectores más vulnerables para asegurar su subsistencia durante la pandemia. Cualquier condicionamiento de acceso a beneficios sociales a la descarga y uso de estas tecnologías debiera encontrarse prohibido, por someter el acceso al auxilio del Estado a la renuncia de derechos en forma discriminatoria con los segmentos más vulnerables de la población, cuyo consentimiento se encontrará completamente viciado. Otro tanto puede afirmarse del condicionamiento de uso de estas aplicaciones para el ejercicio del derecho a movilidad en espacios públicos o acceso a oportunidades de empleo a las que ya me he referido.

Entre lo público y lo privado: derechos humanos como principio guía

Datos de geolocalización en manos las empresas TICs súbitamente aparecen revestidos de un interés público y la disposición de las empresas para colaborar con la autoridad en la provisión de datos útiles al combate de la pandemia debe hacerse bajo el prisma de la necesidad y proporcionalidad planteadas también para los datos en manos de los gobiernos.

La iniciativa de las empresas privadas y la respuesta a los requerimientos provenientes de los estados debe ser evaluada en el marco de los Principios Guía de Derechos Humanos y Empresas de las Naciones Unidas (UNGP). Algunas empresas, como las de servicios móviles agrupadas en la GSMA, así lo han entendido, a través de la publicación de un conjunto de principios orientadores en el requerimiento de datos de usuarias en el contexto de pandemia, al que ya nos hemos referido. En esta misma línea se ubican los esfuerzos de compañías que proveen servicios en Europa y que han intentado colaborar con las autoridades a nivel local y regional, pero sin poner en riesgo la privacidad de sus usuarias.[73]

73 Joakim Reiter, Correct use of telecom data can help in this crisis, Político, 27 de marzo 2020, disponible en: <https://www.politico.eu/sponsored-content/correct-use-of-telecom-data-can-help-in-this-crisis/>

El reposicionamiento de la oferta de tecnologías de vigilancia para el combate de la pandemia es otro aspecto problemático en la colaboración público-privada. En Estados Unidos, Clearview ofrece soluciones de reconocimiento facial previamente desarrolladas con objetivos de seguridad pública para ponerla al servicio de la trazabilidad de contactos. La base de datos de Clearview AI[74] se conforma de imágenes y datos tomados de cuentas de redes sociales, sin el permiso explícito de sus titulares.

Por su parte, Palantir ofrece servicios de inteligencia de datos a las autoridades de salud de Estados Unidos y el Reino Unido.[75] Mientras que NSO —una empresa israelí con un historial previo sumamente problemático, cuyo spyware se ha utilizado contra periodistas y activistas alrededor del mundo— propone reposicionar su tecnología de vigilancia hacia un nuevo producto no militar, que busca establecer trazabilidad de contactos por medio del uso de datos de geolocalización de teléfonos móviles.[76]

Resulta bastante problemático que estas empresas intenten un lavado de imagen con ocasión de la pandemia, que instale relaciones que se proyecten en el tiempo, con tecnologías de vigilancia que puedan ser rápidamente redirigidas a otros fines de control social una vez finalizada la pandemia, con la ventaja de haberse instalado en el ideario de la ciudadanía como dispositivos de protección. Existe un imperativo impuesto por los UNGP de que el despliegue de estas tecnologías de vigilancia se realice previa evaluación de impacto en derechos humanos, que permita a las empresas satisfacer sus tres pilares "proteger, respetar y remediar".

Hablemos de contextos locales

El elefante en la habitación a la hora de evaluar el rol que la tecnología puede cumplir en la mitigación de la pandemia son precisamente las limitaciones de despliegue de la tecnología en determinados contextos y geografías.

No basta que una tecnología se pruebe útil en su capacidad técnica. La pregunta crucial a la hora de tomar decisiones de política pública acerca de su implementación es cuáles son las probabilidades y costos de despliegue de esa tecnología en el breve plazo, que requiere un contexto de pandemia en curso. Países que llevan años luchando por reducir su brecha digital súbitamente caen en la herejía tecno-optimista ignorando la prevalencia de esa brecha, que abarca diversas capas, desde la infraestructura hasta las habilidades digitales disponibles en distintos segmentos de la población.

Partiendo por la conectividad, las tecnologías propuestas deben ser aptas para su despliegue en consideración del acceso a internet o a las comunicaciones móviles, que se pretenden usar como base del despliegue. Con vastos segmentos de población que sufren restricciones de acceso, por razones de infraestruc-

74 Jacob Ward and Chiara Sottile, A facial recognition company wants to help with contact tracing. A senator has questions, NBC News, 30 de abril 2020, disponible en: <https://www.nbcnews.com/tech/security/facial-recognition-company-wants-help-contact-tracing-senator-has-questions-n1197291>

75 Thomas Brewster, Palantir, The $20 Billion, Peter Thiel-Backed Big Data Giant, Is Providing Coronavirus Monitoring To The CDC, Forbes, 31 de marzo 2020, disponible en: <https://www.forbes.com/sites/thomasbrewster/2020/03/31/palantir-the-20-billion-peter-thiel-backed-big-data-giant-is-providing-a-coronavirus-monitoring-tool-to-the-cdc/#43315dd41595>

76 Gwen Ackerman and Yaacov Benmeleh, Israeli Spyware Firm Wants to Track Data to Stop Coronavirus Spreading, Bloomberg Technology, 17 de marzo 2020, disponible en: <https://www.bloomberg.com/news/articles/2020-03-17/surveillance-company-nso-supplying-data-analysis-to-stop-virus>

tura, disponibilidad de servicios por actores comerciales o baja calidad de servicio que interrumpe la calidad de la conectividad, la posibilidad de las tecnologías de alcanzar en forma masiva a la población en el combate a la pandemia se estrecha.

Avanzando un paso más, otro tanto se vincula a la disponibilidad de dispositivos por individuo que permitan asociar la información disponible en éste con su titular. En el mundo y en cada país de América Latina, aún aquellos con mayor nivel de desarrollo, existe un número no reducido de personas que, por edad, condición económica, origen étnico o incluso por factores de género carecen de la posibilidad de acceder y controlar un dispositivo de carácter personal. ¿Qué dirán sus datos? ¿Cómo pueden beneficiarse de una tecnología que los invisibiliza otra vez?

Llegamos a la capa más humana del problema, las habilidades digitales para entender, controlar y generar vínculos de confianza con la tecnología son un obstáculo considerable para ubicarla como una pieza central en la estrategia contra la pandemia.

Ligado con todos los factores anteriores, la efectividad de algunas de las tecnologías propuestas —en particular las de trazabilidad de contactos— descansa en alcanzar un alto nivel de penetración en la población, lo cual resulta poco realista en todos aquellos contextos en que existen barreras considerables en cada uno de los aspectos aquí examinados.

Es en este ingrediente del análisis en el cual la herejía tecno-optimista se manifiesta con mayor fuerza y claridad: la relación de causalidad se encuentra irremediablemente quebrada en un contexto en el cual las múltiples barreras existentes ponen un coto a la utilidad teórica de la tecnología, obligándola a abandonar la soberbia de quienes la predican, no para descartarla, pero sí para reubicarla en el modesto lugar de contribución que le corresponde como coadyuvante en una estrategia más amplia basada en la amplificación de la capacidad humana.

El paradigma político que crea la pandemia: el riesgo y la oportunidad

No han sido pocos los que han insistido en alertar sobre los cambios fundamentales que el rol asignado a la tecnología en pandemia está generando en la narrativa de ejercicio de las libertades públicas.[77]

Las restricciones se visten de un traje blanco metafóricamente equivalente al uniforme que despliegan los heroicos funcionarios de la salud, encargados de los cuidados intensivos de los infectados con el COVID-19. Si la vigilancia que acompaña el despliegue de la tecnología es benévola, qué más da usar la tecnología a la cual el capitalismo de vigilancia ya nos ha acostumbrado, ahora sí para un fin loable: preservar la vida de tantas personas que navegan a oscuras un mar infestado por un enemigo invisible.

El párrafo anterior se excede en metáforas, lo hace a propósito. El discurso que envuelve al despliegue de la tecnología en el contexto de pandemia en tan rico en metáforas que desdibuja esos áridos límites que años de trabajo en estándares internacionales de derechos humanos han intentado plantar como bandera. No suena tan convincente hablar de legalidad, necesidad y proporcionalidad o ponderación de derechos,

77 Evgeny Morozov, The tech 'solutions' for coronavirus take the surveillance state to the next level, The Guardian, 15 de abril 2020, disponible en: <https://www.theguardian.com/commentisfree/2020/apr/15/tech-coronavirus-surveilance-state-digital-disrupt?CMP=share_btn_link

cuando del otro lado se habla de vencer todos juntos al enemigo invisible, de cuidarnos juntos.

Todos somos necesarios en la lucha, la información recolectada para otros usos por agencias públicas o privadas puede ser redirigida para ser usada contra la pandemia, las desconfianzas pasadas en las capacidades y en la probidad de las autoridades deben ser puestas en suspenso, la confidencialidad de los estados de salud puede ser relajada, y las empresas que antes ofrecían tecnología para espiar y amedrentar a periodistas y defensores de derechos humanos, o para ejercer el control discriminatorio de migrantes y minorías étnicas, se les debe conceder el beneficio de la duda, pues ahora sí usarán sus capacidades para el bien público.

Una narrativa de negociación e intercambio (*trade-off*) se instala para conducirnos a la normalización de una vigilancia sin color político, porque todos somos necesarios en la lucha. Pero esta política de la vigilancia al servicio del bien común tiene una víctima y no es el virus. Las capacidades limitadas de la tecnología para contribuir a la mitigación de la pandemia hace más probable que terminen dañando más severamente y a largo plazo a las libertades públicas que al SARS-CoV-2.

Particularmente preocupante es que las tecnologías de vigilancia se desplieguen bajo estatutos de emergencia que apelan a las lógicas de guerra que permiten situaciones de excepcionalidad en los balances y controles de aquellos en el poder público, y que les liberan de la necesidad de la mínima rendición de cuentas, transparencia y supervisión exigibles en otro contexto. Esta narrativa no es completamente nueva; después de unos años de uso intensivo en la lucha contra el terrorismo post 9/11 la tenemos de vuelta, fresca y revigorada por un enemigo invisible aún más fácil de temer y odiar por su ausencia de humanidad.

La tecnología de vigilancia permite decidir quién está autorizado a participar de la vida pública, quién puede trabajar, quién debe quedarse en casa, quién recibe la ayuda económica que le permita sobrevivir y quién no. Nada de eso es propio de una sociedad movida por principios democráticos ni el respeto de los derechos humanos. Más bien, parece un eco de las mejores novelas de ficción que vaticinaban un futuro de autoritarismo y control en nombre del bien público.

Queda claro el riesgo de que estas narrativas asépticas sobre el rol de la tecnología capturen a progresistas y neoliberales bajo la promesa de hacer realidad un mundo en que la autoridad de turno nos lidere a través de la tecnología hacia el futuro escogido para nosotros, por nuestro propio bien. ¿Cuál es la oportunidad entonces? La que nace de ese riesgo. Tenemos frente a nosotros la oportunidad de no dejarnos seducir por la herejía del tecno-optimismo y exigir más de los contextos que acompañan la implementación de la tecnología. Nadie aboga por desterrar a las tecnologías, sino más bien otorgarles el modesto lugar que les corresponde, en un contexto político y normativo que permita poner límites a sus usos y abusos

La pandemia ha reforzado la ubicuidad de la tecnología en nuestras vidas y esta es la mejor oportunidad para entender la necesidad urgente de reclamar de vuelta el control individual y colectivo de aquella que se despliega desde el mundo público y privado en nuestro nombre.

Un camino hacia adelante

Develada la herejía tecno-optimista, Nos toca hacernos cargo de proponer bases sólidas para que el uso de la tecnología en contexto de pandemia se encamine a liberar su máxima potencialidad, por limitada que ella sea, con respeto a los derechos de las personas, cuya protección debe estar estar al centro de la estrategia de mitigación de la pandemia.

Eso requiere que, ya sea a través de una legislación ordinaria o de emergencia, se obligue a que las soluciones tecnológicas que usen datos personales como insumo en el contexto de pandemia satisfagan los siguientes componentes:

1. caracterizar en forma estricta la situación de emergencia y/o el plazo que habilita acceder a los datos personales y sensibles de salud en manos de los distintos órganos del Estado;
2. especificar quiénes estarán a cargo del acceso extraordinario a tales datos;
3. detallar cuáles son y cómo se utilizarán los datos a los cuales se solicita acceso extraordinario. Y, si son recogidos directamente por sus titulares, que ello se realice en forma voluntaria;
4. establecer provisiones de término del acceso y uso extraordinario a los datos, con medidas efectivas de control de acceso o eliminación, en su caso;
5. ordenar medidas específicas de seguridad operacional para evitar acceso y uso malicioso de los datos; y disponer que el uso de los datos personales se haga bajo técnicas de pseudonimización o disociación (con algoritmos de anonimización suficientemente robustos) cuando se trate de ofrecer información públicamente disponible, además de tener la seguridad como requisito indispensable, incluyendo el tránsito cifrado de la información y su almacenamiento seguro y resiliente;
6. garantizar la representatividad de los datos de los cuales se nutre la tecnología y la toma de decisiones de políticas públicas que ella alimenta, teniendo consideración con los contextos locales que dan cuenta de la marginalización de grupos vulnerables;
7. establecer mecanismos de evaluación de la tecnología implementada, en su efectividad y precisión técnica, pero también en su impacto en el ejercicio de derechos humanos y no solo privacidad; y,
8. establecer mecanismos de transparencia, control externo y rendición de cuentas que permitan fiscalizar y sancionar fuertemente la desviación de finalidad en el acceso y uso de los datos.

Estos controles y contrapesos nos devuelven a nuestros viejos y conocidos estándares de legalidad, necesidad y proporcionalidad en la limitación del ejercicio de derechos humanos que siguen constituyendo una obligación positiva de promoción y protección de los Estados en el contexto de pandemia. Aquí la vacuna no necesita ser inventada, se encuentra disponible en los estándares internacionales de derechos humanos del Sistema Universal y del sistema Interamericanos de Derechos Humanos.[78]

No dejemos que la herejía tecno-optimista que florece en pandemia nos confunda con su perfume.

78 Comisión Interamericana de Derechos Humanos, Resolución 1/20. Pandemia y Derechos Humanos en las Américas, 10 de abril 2020, disponible en: <https://www.oas.org/es/cidh/decisiones/pdf/Resolucion-1-20-es.pdf>


DERECHOS
DIGITALES
América Latina