F·ILIA
Revista No. 2
II semestre
Guayaquil, Ecuador
octubre 2020
ISSN: 2697-3596

COVID-19, tecnología y poder: los peligros del optimismo tecnológico y el surgimiento del omnióptico global

Henry Chávez
PhD en Socioeconomía
CTS-Lab FLACSO Ecuador
/ Pontificia Universidad Católica del Ecuador
henry.chavez@gmx.com
Jacqueline Gaybor
PhD en Estudios de Desarrollo
ISS-Erasmus University Rotterdam, Holanda
gaybortobar@iss.nl

Resumen
En medio de la crisis de COVID-19, los países enfrentan la necesidad de restringir la movilidad para reducir la propagación del virus. Ante la urgencia, varios gobiernos alrededor del mundo, entre esos el Ecuador, están empezando a implementar nuevos mecanismos de control basados en tecnologías de Big Data e inteligencia artificial. Sin embargo, la rapidez de estas decisiones y la falta de reflexión y debate sobre sus posibles consecuencias a corto y largo plazo puede llevarnos a engendrar una nueva estructura de poder y control, construida sobre la base de nuestros propios

Recibido: 17 de junio de 2020 / Aceptado: 31 de agosto de 2020

rastros digitales. Esta nueva estructura puede transformar radicalmente la relación entre Estados y ciudadanos y dar paso a la instauración de regímenes cada vez más autoritarios alrededor del mundo.
Palabras claves: COVID-19, Corona-Apps, vigilancia, optimismo tecnológico, omnióptico.

Abstract
Amid the COVID-19 crisis, countries face the need to restrict mobility to reduce the spread of the virus. Given the urgency, several governments around the world, including Ecuador, are starting to implement new control mechanisms based on Big Data and artificial intelligence technologies. However, the speed of these decisions and the lack of reflection and debate on their possible consequences in the short and long term may lead to the production of a new structure of power and control, built on our digital traces. This new structure can radically transform the relationship between states and citizens and pave the way to the establishment of increasingly authoritarian regimes around the world.
Keywords: COVID-19, Corona-Apps, surveillance, technological optimism, omnioptic.

Introducción

Entre marzo y junio de 2020, varios gobiernos y empresas alrededor del mundo desarrollaron e introdujeron aplicaciones móviles para intentar controlar la propagación de la pandemia de COVID-19. La rapidez del contagio y el número de fatalidades por la crisis sanitaria han llevado a los gobiernos a tomar decisiones con consecuencias inciertas. Su argumento ha sido que se debe actuar rápida y decisivamente. La presión por respuestas inmediatas ha dejado poco espacio para examinar detenidamente los riesgos asociados al despliegue de estas innovaciones tecnológicas que se ofrecen como la mejor solución para frenar la curva de contagio.

Este artículo intenta hacer un análisis crítico al optimismo tecnológico detrás del desarrollo de estos y otros dispositivos que se han implementado a escala global durante

la pandemia. Buscamos identificar y discutir los posibles riesgos y consecuencias, intencionales o inadvertidas, que pueden derivar del uso de estos y de las formas en que están siendo implementados. Si bien partimos de una perspectiva global, pondremos particular atención al caso ecuatoriano, por tres razones. La primera es la necesidad de reflexionar sobre los graves riesgos que implica la adopción de estas aplicaciones en un país donde no existe un marco legal específico de protección de datos personales y privacidad. Hasta la fecha no hay claridad sobre cómo se gestionan los datos personales que se recolectan a través de estas aplicaciones. Adicionalmente, el desarrollo, implementación y uso de estas tiene lugar en el marco de un estado de excepción[1] que limita las posibilidades de discusiones técnicas y democráticas que deberían anteceder a la implementación de estas políticas y tecnologías. La segunda, y este es el argumento central de este artículo, es que el conjunto de políticas, medidas y dispositivos desplegados durante la pandemia revelan un proceso de profunda transformación en la arquitectura de poder a escala planetaria, de la cual el Ecuador también forma parte. Las decisiones que se han tomado desde el inicio del estado de excepción no solo modificarán la forma de gestionar esta crisis sanitaria, sino también la sociedad en que habitaremos. Finalmente, la tercera razón tiene que ver con la urgencia de emprender una discusión crítica y constructiva sobre las políticas públicas en esta materia desde diversos sectores. Creemos que es fundamental preguntarse: ¿dónde se está trazando la línea divisoria entre la seguridad y la protección de la privacidad, y con ella de la democracia y los derechos inviduales?

1 El estado de excepción en Ecuador entró en vigencia el 16 de marzo de 2020 (decreto 1017) y fue extendido primero hasta el 15 de junio de 2020 (decreto 1052); luego, un nuevo decreto que rige hasta el 15 de agosto (decreto 1074).

Enfermedad, tecnología y poder: algo de historia

Si bien la escala y la rapidez de propagación de esta pandemia puede resultar sorprendente, no es la primera vez que el mundo enfrenta una emergencia sanitaria de este tipo. Es necesario dar una mirada a la historia para ver cómo la humanidad ha respondido a episodios similares en el pasado y qué consecuencias tuvieron esas respuestas. Una primera constatación de este ejercicio es que el surgimiento y transformación de prácticas, imaginarios e instituciones se entrelaza con episodios de enfermedades mortales y plagas que han diezmado poblaciones, países e incluso han extinguido culturas y naciones enteras (Foucault 2004; Hildesheimer 1993; Latour 2001). Estos episodios han determinado el desenlace de guerras, conquistas y otras transformaciones sociales fundamentales en la historia mundial. Basta con dar una mirada a los relatos sobre la peste negra, llevada por los mongoles hasta las puertas de Europa y esparcida en el resto del continente por los comerciantes venecianos (Sallmann 2011); la aniquilación de las poblaciones indígenas americanas con la viruela o la sífilis traída de vuelta a Europa por los mismos colonizadores (Diomedi P. 2003; Nunn 2010; Quétel 1984); las diferentes oleadas de cólera, fiebres y plagas entre los siglos XVI y XIX o la gripe española llevada por las tropas americanas a Europa durante la Primera Guerra Mundial (Hildesheimer 1993; Beauvieux 2012; Bouron 2009; Blickle 2020; Sardon 2020). En cada uno de estos episodios, bacterias o virus, estos insignificantes seres (Žižek 2020) crearon las condiciones para el surgimiento de varios dispositivos e instituciones que se han convertido en las bases mismas de los Estados modernos.

Censos, cuarentenas, hospitales, registros biométricos e incluso castigos por desobediencia, son dispositivos que fueron concebidos en un inicio para controlar la propagación de

enfermedades durante diferentes episodios de contagio masivo (Foucault 1975; 2007). Sin embargo, una vez superadas dichas crisis, estos dispositivos fueron conservados e instrumentalizados por los gobiernos para tener un mejor control de sus poblaciones y territorios. Estos dispositivos dieron lugar a la configuración de lo que Foucault denominó un modelo disciplinario de poder basado en tres principios: exclusión, individualización y vigilancia (Foucault 1975). Dicho modelo, fundado en una arquitectura panóptica (Bentham 1995) de las sociedades e instituciones, ha funcionado, se ha perfeccionado y extendido por todo el mundo desde el siglo XIX.

Sin embargo, ese modelo disciplinario resulta hoy insuficiente para mantener el control sobre poblaciones locales en un sistema global cada vez más interconectado y complejo. En ese sentido, la cuarentena global que hemos experimentado marca en realidad un retroceso que podría derivar en la desarticulación del modelo disciplinario que sostiene a los Estados modernos. Esta desarticulación no significa que la disciplina o el control sobre las poblaciones vaya a reducirse, sino probablemente lo contrario. Frente a la pérdida de *soft power* que ofrecía el modelo panóptico, los Estados se ven obligados a buscar nuevas formas de control más invasivas o represivas. La cuarentena y la declaratoria de estados de excepción alrededor del mundo evidencian este proceso.

Pero existe otra tendencia derivada de esta crisis sanitaria que resulta más preocupante: el despliegue de nuevas formas y dispositivos tecnológicos de control y vigilancia de la población. La particularidad de estas tecnologías y el motivo por el que su adopción irreflexiva, apresurada y generalizada resulta preocupante para la democracia radica en su capacidad sin precedentes para remodelar prácticas, imaginarios y políticas a escala planetaria y en muy corto tiempo. Además, como la historia de las epidemias nos muestra, los

dispositivos y formas de control poblacional que se introducen durante este tipo de eventos rara vez desaparecen. Por el contrario, tienden a perennizarse e integrarse a la panoplia de instrumentos de control y disciplinamiento de las poblaciones con los que cuentan los Estados. Cómo se explica entonces que en pleno siglo XXI hayamos recurrido a una tecnología del siglo XIV: la cuarentena. Si esta tendencia se repite, este despliegue de nuevas tecnologías podría ser el indicador del surgimiento de un nuevo modelo de poder.

Las 'Corona' Apps y los límites del optimismo tecnológico

La recolección masiva de datos personales, biométricos, de geolocalización e imágenes a través de cámaras de vigilancia, drones, teléfonos móviles, GPS, Bluetooth y otros dispositivos no es nueva. Sin embargo, se ha intensificado en los últimos años gracias a los avances logrados en los campos de la inteligencia artificial y las tecnologías de Big Data. El rol que han jugado China y varios de sus vecinos asiáticos en el desarrollo de estas tecnologías ha sido fundamental. Es importante resaltar este hecho por dos razones. En primer lugar, estos países fueron los primeros en recurrir a soluciones basadas en este tipo de tecnologías para intentar frenar la propagación de una pandemia cuyo epicentro fue precisamente China. En segundo lugar, esto resulta relevante porque dichos países mantienen en mayor o menor grado sistemas políticos autoritarios que les han permitido desarrollar y desplegar este tipo de tecnologías sin mayor resistencia ni regulación democrática. Este hecho, no menor, ha determinado que el desarrollo de estos dispositivos siga una trayectoria marcada por la impronta de imaginarios y necesidades propias de sistemas políticos altamente jerarquizados y fundados en el control disciplinar de sus poblaciones.

Entre la panoplia de dispositivos tecnológicos que estos países asiáticos desplegaron durante esta crisis, quizás los más populares son las aplicaciones móviles. En efecto, con ciertas variaciones y grados de sofisticación más o menos importantes, casi todos los países afectados por la pandemia han desarrollado este tipo de aplicaciones (Gráfico 1).

Gráfico 1: Corona-Apps disponibles en Google Play por país[2]

En términos generales, estas aplicaciones se enfocan en recolectar tres tipos de información: datos médicos y biométricos, datos de localización y movimiento, y datos de contactos e interacciones. Ante la urgencia y la falta de mejores respuestas a la pandemia, varios gobiernos del norte y sur global vieron en el ejemplo asiático un modelo a seguir. Sin embargo, el nivel de debate crítico sobre su implementación ha variado notablemente de país a país. En varios países europeos, por ejemplo, se ha generado un gran debate sobre sus dificultades técnicas, éticas y legales. Esto se entiende dados los límites que impone el Reglamento General

2 Versión interactiva: http://divergencelab.org/wp-content/uploads/2020/10/covid.html Fuente: Google Play.

de Protección de Datos (RGPD-UE), mismo que da prioridad a la anonimización y la privacidad. A pesar de contar con este sólido marco jurídico común, estos países se han visto obligados a elegir entre 'ceder' y hacer caso omiso de las complejidades que las soluciones tecnológicas imponen a los derechos de privacidad para contener la propagación del virus, o proteger los derechos de sus ciudadanos a la privacidad, la protección de sus datos personales y el futuro de sus democracias.

Sin embargo, en contextos cuyos marcos jurídicos sobre protección de datos y privacidad son más débiles o inexistentes, vemos cómo se despliegan este tipo de tecnologías con mucha rapidez. Pero, debido a restricciones técnicas y financieras, la mayoría de las aplicaciones desarrolladas en o para estos contextos se han enfocado en la recolección del primer tipo de información: datos médicos y biométricos. Este tipo de aplicaciones son promocionadas como herramientas para la autoevaluación médica, por ejemplo: Cuidar (Argentina), CoronApp (Chile), SaludEC (Ecuador), entre otras. En términos generales, estas aplicaciones piden al usuario ingresar cierta información médica y personal. A partir de esta información, evalúan la probabilidad de que la persona esté o no infectada o los riesgos que tiene de contraer el virus. Algunas también dan acceso a información sobre la distribución geográfica del brote del virus. Sin embargo, si tomamos en cuenta la finalidad de las aplicaciones, la pertinencia de la serie de datos personales que estas apliaciones solicitan para su funcionamiento resulta por lo menos cuestionable. Cuidar, por ejemplo, requiere como información obligatoria: el número número de identificación nacional, el correo electrónico y el teléfono. CoronApp va más allá y pide además el número de registro fiscal, edad, dirección, geolocalización, medicamentos que usa, preexistencias de enfermedades, historial de viajes y contactos. SaludEc solicita información personal, datos de geolocalización del teléfono, lista

de redes wifi-circundantes, número de cédula, correo electrónico, ciudad, dirección de residencia y teléfono. En ninguno de estos casos se estipula claramente cuál es la necesidad de recolectar todos estos datos para producir un 'autodiagnóstico', objetivo principal de estas aplicaciones.

El segundo tipo de aplicaciones, basadas en la recolección de datos de geolocalización, apunta a limitar o gestionar la libertad de movimiento de las personas durante las cuarentenas. En Taiwán, por ejemplo, esta función ha sido uno de los pilares fundamentales de la gestión de la crisis. Un sistema que no ha pasado inadvertido, ya que les ha permitido controlar a la población a través de multas a quienes incumplen el aislamiento (Cole 2020). Las aplicaciones funcionan como una «cerca electrónica invisible» que monitorea las señales telefónicas para alertar a la policía si la persona que está en cuarentena se aleja de su dirección o apaga su teléfono. En algunos países, como Australia, Rusia, Estados Unidos, estas aplicaciones funcionan junto con brazaletes electrónicos con capacidad de rastreo GPS (Bakkemo 2020; Fernandes 2020; Satter 2020). Algunas empresas privadas en el sur global también han diseñado estrategias para controlar el cumplimiento del aislamiento preventivo y obligatorio. La compañía argentina Urbetrack, por ejemplo, diseñó Cuídate En Casa (Infobae 2020), una aplicación que trata de emular a la experiencia taiwanesa. Esta trabaja con dependencias gubernamentales y fuerzas de seguridad para monitorear la movilidad de las personas que incumplen cuarentenas.

Un tercer tipo de aplicaciones usan el rastreo de contactos para indicar si hay riesgo de contagio sobre la base de datos de interacción y proximidad con personas diagnosticadas con COVID-19. El rastreo de contactos puede usar diferentes tipos de tecnología de ubicación. Por ejemplo, la aplicación TraceTogether de Singapur funciona a través de Bluetooth. Otras aplicaciones usan también tecnología GPS, como la noruega Smittestopp

(Nikel 2020) o la surcoreana Self-quarantine Safety protection (Kim 2020). Pero, el uso de este tipo de tecnologías, que daría poder a los Estados para rastrear y almacenar las ubicaciones de sus ciudadanos y sus contactos, ha activado varias alarmas y generado un fuerte debate al interior de varios países. Para saldar este asunto, varios gobiernos europeos encargaron a grupos de expertos, científicos, empresas y organismos de protección y control de datos y privacidad para que diseñen posibles soluciones que se apeguen a las normativas europeas (PEPP-PT 2020; Untersinger 2020b; Miller y Chazan 2020). Entre los puntos centrales de este debate se encuentra el carácter centralizado o descentralizado de los sistemas que se implementen, su interoperabilidad entre países, la seguridad de los datos y los mismos sistemas, el anonimato, el carácter voluntario de su uso y ciertas consideraciones sobre la soberanía de los Estados europeos frente al poder de compañías como Apple y Google (Gebhart y Cyphers 2020; Kobeissi 2020; Miller y Chazan 2020; Untersinger 2020a; 2020b; Untersinger y Breteau 2020). En efecto, estas últimas lanzaron en abril una herramienta común a ambos sistemas operativos para que pueda ser utilizada por cualquier empresa o Estado que desarrolle aplicaciones de trazado de contactos por Bluetooth (Girard 2020). La herramienta propuesta por las empresas estadounidenses opta por un sistema descentralizado en la que, en principio, ninguna información personal del usuario es compartida ni con el Estado, ni con dichas empresas. El principio es simple: cada teléfono emite códigos aleatorios que son captados por los teléfonos de otras personas que se encuentren cerca y los almacenan localmente. Cuando una persona es diagnosticada positivo con COVID-19, este lo notifica en la aplicación y los códigos emitidos por su teléfono son transmitidos a la red de usuarios para que cada teléfono verifique si alguno de esos códigos coincide con los que tiene almacenados localmente. Sin embargo, este esquema aparentemente respetuoso

de la privacidad tiene sus bemoles ya que resulta más vulnerable a ataques informáticos malintencionados, reporte de falsos positivos, rastreo dirigido, la anonimidad puede fácilmente ser vulnerada, etc. (Miller y Chazan 2020). Sobre la base de algunos de estos argumentos, equipos como el del Institut National de Recherche en Informatique et Automatique (INRIA) de Francia han desarrollado sistemas de tipo centralizado (Robert) en el que los códigos generados por cada teléfono son manejados por un sistema central que distribuye y anonimiza los códigos de los usuarios. En este modelo, los usuarios solo comparten sus datos con el servidor central y no con toda la red, lo cual reduce las posibilidades de identificación de los usuarios, pero, en cambio, se da por supuesto que quien maneja el servidor central es un ente de confianza. Esta es precisamente una de las mayores críticas a este sistema ya que este supuesto es fácilmente quebrantable (Gebhart y Cyphers 2020; Kobeissi 2020). Si bien el debate técnico, legal y ético alrededor de estos dispositivos no ha sido resuelto y las críticas a ambas soluciones siguen sin respuesta, la urgencia de retomar las actividades económicas ha empujado a los gobiernos a lanzar sus propias aplicaciones. Francia optó por un sistema centralizado: StopCovid (Escande 2020); mientra que Alemania por uno descentralizado: Healthy Covid (Lyons 2020).

Por último, hay aplicaciones que recolectan y usan los tres tipos de información. La aplicación china Alipay HealthCode app, por ejemplo, combina el uso de información biométrica, rastreo de los movimientos y el rastreo de contactos (Mozur, Zhong, y Krolik 2020). Esta aplicación asigna a los usuarios tres códigos de color basados en su estado de salud y su historial de viajes. Además, genera un código QR que puede ser escaneado por las autoridades policiales. La aplicación tiene especificidades de acuerdo a cada ciudad, pero los 3 códigos de color son una característica común. El código verde permite el movimiento con relativa libertad, el amarillo indica estar en aislamiento doméstico, y el

rojo designa un caso confirmado de COVID-19 que debería estar en cuarentena. La aplicación se basa en información ingresada por el usuario, pero también en la información suministrada por el gobierno. Esto comprende los registros médicos, el historial de viajes y la información sobre el contacto con alguien a quien se le ha diagnosticado COVID-19. Sin embargo, la aplicación no deja claro a sus usuarios qué datos están siendo recolectados y almacenados, quién puede usarlos, ni tampoco su relación con las autoridades encargadas de hacer cumplir la ley. Los abusos y riesgos que este tipo de tecnologías pueden traer no son menores en contextos autoritarios como el chino, donde además su uso es obligatorio. Basta con imaginar la facilidad con que estas tecnologías pueden limitar la movilidad de un ciudadano o su capacidad para acceder a bienes, servicios u otros derechos.

Sin embargo, a pesar de las promesas y la proliferación exponencial de estas aplicaciones, su verdadera utilidad y efectividad en la lucha contra la pandemia resulta cuestionable. El gráfico 2 muestra que, hasta junio 2020, de las 217 aplicaciones disponibles en el mundo solo 27 han sido instaladas por más de 1 millón de usuarios y apenas 4 por más de 5 millones. Cuidar (Argentina), CoronApp (Colombia), Hayat Eve Sığar (Turquía) y Ada (Alemania). Dos excepciones sobresalen: Aarogya Setu (India), con más de 100 millones de usuarios y Caixa (Brasil), con 50 millones de usuarios. El número de usuarios en esta última se explica porque es una aplicación de ayuda financiera para los trabajadores informales durante la pandemia (Sputnik 2020). No obstante, incluso en estos dos últimos casos, el número de usuarios representa apenas 7 % y 23 % de sus poblaciones, respectivamente. Ahora bien, solo en el caso de las aplicaciones de *contact-tracing*, las más sofisticadas y que en teoría podrían ayudar a reducir el contagio, se estima que al menos un 60 % de la población debería usarlas para que tengan alguna efectividad (Castañeda y Toledo 2020; Miller y Chazan 2020; Busvine 2020).

Estas estimaciones suponen además que la detección de personas infectadas y la tecnología de *tracing* funcionan al 100 %. Siguiendo el modelo de Ferretti et al. (2020), con una efectividad del 50 % en el sistema de test y de identificación de contactos y un 20 % de la población usando este tipo de apliaciones, su efectividad se reduce al 1 %. Si dichas estimaciones son correctas, el despliegue de este tipo de dispositivos hasta la fecha tendría poco o ningún efecto concreto en el control de la pandemia.

Estos datos ponen en evidencia los límites del optimismo tecnológico y una cierta tendencia general entre los tomadores de decisión alrededor del mundo a operar desde mecanismos propios del pensamiento mágico (Stivers y Stirk 2001; Chávez 2017; Chávez y Gaybor 2018; Jasanoff y Kim 2015). Pero, lo más preocupante no es la falta de racionalidad en los dirigentes políticos, sino los riesgos para la democracia y los derechos individuales que la adopción apresurada de estas 'recetas mágicas' está generando alrededor del mundo. Si bien ninguna de esas aplicaciones alcanza por sí sola una masa de usuarios mínima para cumplir la función para la que fueron creadas, la información recolectada por cada una de ellas —datos personales, clínicos, de localización, contactos, entre otras— suma ya una base de datos de alrededor de 190 millones de personas. Esta información puede no ser suficiente para detener la pandemia, pero bien podría ser muy efectiva para otros propósitos como restringir el acceso a seguros de salud, a empleos o controlar poblaciones. La falta de transparencia, y sobre todo de regulaciones locales en materia de protección de datos y privacidad en las que estas aplicaciones fueron desplegadas, levanta varias alarmas sobre la gestión que se dará a toda esta información y los posibles usos que puedan darle gobiernos o empresas privadas. Basta con recordar algunos casos recientes de fuga, robo, exposición o venta de bases de datos con información sensible en Ecuador (Plan V 2019), Chile (Cifuentes 2018; Cortes 2019), Perú (Hautala

2020), México (Heran 2018) y de varias plataformas que operan en todo el mundo como Waze, Linkedln, iCloud, Adobe, Uber, Netflix, Zoom o Facebook (Abrams 2020; Bischoff 2019; Cimpanu 2019; El Colombiano 2016; Galvan 2019; Jee 2019; McCormick 2014; Musil 2019). El caso de Facebook resulta emblemático por su relación con el escándalo de Cambrigde Analítica que puso en evidencia el poder de las tecnologías de Big Data para manipular la opinión de los ciudadanos e influir en procesos electorales alrededor del mundo, entre ellos la elección de Donald Trump y el Brexit (Lapowsky 2018; 2019; Amer 2019). Este escándalo ejemplifica la gravedad del riesgo que introduce la creación indiscriminada y desregulada de bases de datos con información sensible para la democracia y los derechos individuales.

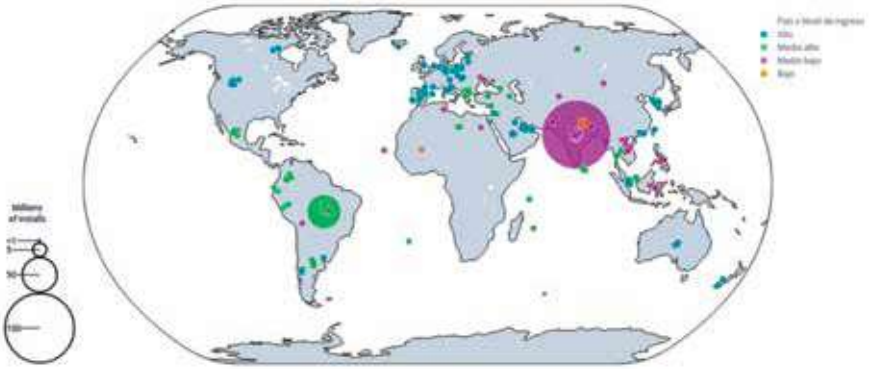

Gráfico 2: Número de descargas de Corona-Apps para Android por país[3]

La falta de regulación sobre la gestión de los datos y los riesgos para la privacidad: caso Ecuador

Como otros gobiernos del Sur Global, Ecuador se ha adherido a la fórmula que combina el aislamiento social con la detección temprana y el rastreo de infectados a través de aplica-

3 Versión interactiva: http://divergencelab.org/wp-content/uploads/2020/10/covid2.html. Fuente: Google Play.

ciones móviles. Por el momento, el gobierno ha desarrollado dos aplicaciones: SaludEC y CovidEC.[4] Estas sirven principalmente para la autoevaluación médica y geolocalización. Básicamente solicitan al usuario cierta información médica y sobre esta base evalúan si es probable que esté infectado. Si es el caso, dan ciertos consejos de cómo gestionar la enfermedad y qué acciones tomar. Estas aplicaciones también dan acceso a información geográfica sobre el brote del virus a través de mapas.

Sin embargo, como ya se mencionó, estas aplicaciones solicitan una serie de datos personales cuya pertinencia no siempre queda clara. SaludEC, por ejemplo, requiere como información obligatoria el número de cédula, correo electrónico, ciudad, dirección de residencia, teléfono, fecha completa de nacimiento y aceptación de las condiciones de uso. Dichas condiciones establecen, entre otras cosas, que el Ministerio de Salud Pública y otras instituciones del Estado pueden contactar al usuario «por medio de WhatsApp, SMS, correo electrónico y otros medios digitales con información oficial». Adicionalmente, la aplicación puede acceder a la ubicación determinada por GPS y por las redes cercanas; a las fotos, multimedia y archivos —pudiendo leer y además modificar o eliminar el contenido almacenado—; a la información sobre la conexión WIFI y el acceso completo a las redes.

Esta solicitud de datos personales para la habilitación y uso de aplicaciones no es anodina. Es en realidad producto de los imaginarios movilizados por las mismas autoridades públicas que las promueven. En la presentación pública de SaludEc, por ejemplo, Andrés Michelena, ministro de Telecomunicaciones del Ecuador, presentó la entrega de datos personales como algo intrascendente, una simple etapa de rutina para descar-

4 Esta app, específicamente, fue diseñada por el Ministerio de Telecomunicaciones y de la Sociedad de la Información.

gar y utilizar la aplicación (Teleamazonas 2020). Este tipo de discurso oficial endosa un nivel incuestionable de confianza a estas aplicaciones mientras que nos deja ver la falta de visión crítica de la clase gobernante sobre los efectos que esto tiene para sus ciudadanos y la misma responsabilidad de los entes públicos. El riesgo potencial relacionado con la seguridad y la privacidad es inadvertido y además cobijado en la idea de garantizar el bien común en una situación de miedo generalizado por efecto de la pandemia.

Sin embargo, estos peligros se hacen cada vez más tangibles. Anomali Threat Research, compañía estadounidense dedicada a la ciberseguridad, ha detectado hasta el momento al menos una docena de aplicaciones falsas. Estas aplicaciones están diseñadas para parecerse a las herramientas oficiales de lucha contra la pandemia y a través de las cuales es posible robar identificadores y datos personales (Suazo 2020). Así mismo, Amnistía Internacional alertó que aproximadamente los datos de un millón de usuarios de la aplicación de contact tracing desarrollada por Qatar (Ehteraz) habían sido expuestos a posibles hackeos (Hern 2020). Y no podemos olvidar que el 16 de septiembre de 2019 ocurrió la mayor filtración de datos en la historia del Ecuador. Esta dejó expuesta información personal[5] de más de 20 millones de ecuatorianos (vivos y muertos), proveniente del Registro Civil, el Instituto Ecuatoriano de Seguridad Social, el Banco de Instituto de Seguridad Social, entre otros. Esta información incluía, por ejemplo, datos sobre estados de cuenta y créditos de las personas (Cadena 2019). Las consecuencias de este evento ponen de manifiesto el grave riesgo que enfrentamos al entregar nuestros datos personales. De igual

5 Nombres y apellidos, número de cédula, RUC, género, fecha y lugar de nacimiento, dirección de residencia, correo electrónico, números telefónicos, estado civil, nivel de educación, entre otros.

manera, el 22 de marzo 2020, en plena pandemia, se filtró información confidencial desde el municipio de Quito sobre la distribución por sectores de casos de personas contagiadas (Carvajal 2020).

Pero no solo el gobierno promueve aplicaciones para la autoevaluación y monitoreo de zonas con casos confirmados o con riesgo de contagio. El departamento de modelización matemática de la Escuela Politécnica Nacional también diseñó la aplicación Salvavidas. Esta permite acceder a información sobre la distribución y patrones de dispersión geográfica de los casos confirmados y de zonas con mayores probabilidades de contagio de COVID-19. Según las declaraciones a un medio local de uno de los creadores de esta app, la urgencia es tal, que sin estas aplicaciones:

> La sociedad se va romper, si nosotros seguimos encuarentenados todo el tiempo se va a romper, no vamos a tener qué comer, no vamos a tener salario y la cosa se va a romper; en Italia hay saqueos, también tenemos que precautelar la sostenibilidad del país (*El Universo*, 2020).

Como en otras partes del planeta, este tipo de declaraciones evidencia cómo el uso de estas aplicaciones es percibido, desde un optimismo tecnológico acrítico, como la 'solución mágica' para detener la pandemia y evitar los escenarios catastróficos imaginados o movilizados por los tomadores de decisiones para justificar su adopción.

Las apps de COVID-19 diseñadas en Ecuador recopilan una serie de datos personales cuyo propósito o función no esta claro. Salvavidas, por ejemplo, cuyo objetivo es «identificar patrones de propagación de la enfermedad», requiere para su utilización que el usuario provea información personal sobre su historial de salud. Preguntas como ¿tiene usted cáncer?,

¿padece de problemas cerebrovasculares?, ¿padece de problemas coronarios?, ¿tiene diabetes? son indispensables para realizar el llamado 'autotest'. Esta información tiene poca o ninguna relevancia para visualizar las zonas de riesgo de contagio, conocer el cerco epidemiológico, u obtener un diagnóstico médico del COVID-19. Puede, sí, indicar el riesgo que una persona tiene de desarrollar un cuadro grave de la enfermedad. Pero esa información, el usuario la puede conocer sin tener que poner su información personal en una base de datos que puede terminar en manos de terceros y limitar sus derechos sociales, económicos y políticos.

En una entrevista radial realizada a uno de los creadores de la aplicación Salvavivas, este señaló sobre la protección de la privacidad que:

> Nosotros tenemos algunos escudos [...] para que nuestros servidores y computadores en los cuales está almacenada la información no sean vulnerados. [...] Pero, la otra cosa también es por supuesto, una confianza que se le da a la institución, en este caso al centro de modelización de la Politécnica Nacional y es una confianza en ese sentido. [...]. Hay una confianza en que la gente de la institución no va a usar mal la información. Nuestro propósito como institución de educación superior no es lucrar, por supuesto que no. Es más bien tener una herramienta de ayuda para la ciudadanía (Majestad FM, 2020).

Esta declaración devela el deseo de contribuir a la comunidad detrás de la innovación tecnológica. Sin embargo, este voluntarismo se sostiene sobre la idea bastante cuestionable de que la entrega de datos personales se la hace como un gesto de 'confianza' en una institución de educación superior que no tiene ánimos de lucro. Esta visión minimiza la responsabilidad

sobre la gestión de esos datos únicamente a través de 'herramientas tecnológicas'. Adicionalmente, este discurso demuestra que hay un paso previo que no ha sido previsto: garantizar el principio de la limitación a la recopilación y al procesamiento de datos personales, el cual debe ser proporcional al fin legítimo perseguido. Este es un principio reconocido, por ejemplo, en el RGPD-UE. La entrevista denota la falta de un marco jurídico en el Ecuador que determine los principios básicos de la protección a la intimidad, donde debe destacarse la limitación a recopilar y procesar datos y a esto sigue el determinar la responsabilidad legal sobre su tratamiento, el cual tiene que ver con el acceso, seguridad, conservación, transferencia o eliminación de estos datos.

Tal vez, antes de lanzar más de estas aplicaciones que ponen en riesgo no solo a los ciudadanos como individuos, sino a la democracia, cabría preguntarse primero si estas cumplen realmente la función para la que fueron creadas y segundo, cómo garantizar su funcionamiento y la protección de sus usuarios en contextos como el Ecuador. La aplicación SaludEc, por ejemplo, es promocionada como facilitadora para brindar atención especializada a través de telemedicina, agendar una cita médica en establecimientos de salud pública o servir de enlace inmediato para una atención urgente con el 911 (FM Mundo 2020). Pero si la aplicación sirve para lo mismo que se podría hacer a través de una llamada al 171 o al 911, ¿qué utilidad real tiene para el usuario?

Por otro lado, según el reporte *Digital 2020: Ecuador* (Hootsuite y We are social 2020), si bien el 89 % de la población ecuatoriana tienen un teléfono celular, solo el 66 % de estos son Smartphone. El 69 % de la población tiene internet, pero solo el 23 % del tráfico se da través de un teléfono. Esto se explica ya que el 74 % de las conexiones telefónicas en el país son prepago y tienen acceso limitado a otros ser-

vicios de internet que no sean Facebook o WhatsApp, que se ofrecen gratuitamente con dichos planes. Otro aspecto a considerar es que el 86 % de los teléfonos inteligentes en el país usan Android como sistema operativo, lo cual plantea algunas preguntas sobre las posibilidades reales de conseguir un uso extendido de estas aplicaciones, considerando los problemas de compatibilidad que se presentarán en el corto y mediano plazo.

Sin lugar a duda, algo que debería anteceder la puesta en marcha de estas aplicaciones es la discusión sobre privacidad y protección de datos. Si bien este no ha sido el caso en el Ecuador, el contexto de esta pandemia nos empuja y señala la urgencia de navegar la inevitable tensión entre balancear derechos individuales (como el derecho a la intimidad y la protección de datos personales) frente al amparo de intereses comunitarios relacionados con la salud pública y beneficiar significativamente la vida de los ciudadanos. En la esfera de la salud pública, este debate no es nuevo (Bayer y Fairchild 2002; Myers et al. 2008). La filtración, transferencia o entrega de datos personales ligados con enfermedades venéreas, diabetes, tuberculosis (Fairchild, Colgrove, y Bayer 2003) y VIH (Bayer y Fairchild 2002) a personas fuera de la comunidad médica y con propósitos diferentes a los cuales los datos fueron recolectados, ha sido sujeto de disputa incluso antes de la digitalización de la información. En particular, cuando no se ha determinado bajo qué circunstancias los datos personales pasan a ser datos públicos y las obligaciones y responsabilidades que esto conlleva. La preocupación con respecto a la afectación del derecho a la privacidad adquiere otro nivel de complejidad al verse mediado por el componente digital. Además, esto se vuelve incluso más complicado en un contexto como el ecuatoriano, donde, al igual que en otros países de la región,

no hay un marco regulatorio específico[6] para la protección de datos personales y la intimidad.

La situación que vive el Ecuador en medio de un estado de excepción es compleja. El artículo 11 del Decreto Ejecutivo N.º 1017 dispone que «se podrán usar 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». El 19 de marzo de 2020, la Corte Constitucional del Ecuador emitió el Dictamen No. 1-20-EE/20, favorable al Decreto Ejecutivo. Respecto del artículo 11, la Corte precisó que el uso estas tecnologías «es una medida idónea, necesaria y proporcional, debido a que optimiza los recursos humanos y materiales para lograr los fines del estado de excepción declarado». La Corte, sin embargo, resalta que dicha utilización no debe ser un medio para la transgresión de los derechos a la privacidad, a la no discriminación y a la protección de los datos personales de las personas examinadas sanitariamente durante la pandemia. Ahora bien, un elemento importante del dictamen de la Corte es la limitación del uso de estas herramientas tecnológicas solo a «aquellas personas a quienes las autoridades de salud han dispuesto de manera específica el aislamiento voluntario u otras medidas de similar naturaleza». A su vez, estas personas deben ser debidamente informadas sobre esta medida y su alcance.

6 La Declaración Universal de Derechos Humanos establece las bases del derecho humano a la intimidad en su artículo 12. Otros instrumentos internacionales como el Pacto Internacional de derechos civiles y políticos (artículo 17, numeral 1) y la Convención Interamericana de Derechos Humanos (artículo 11, numeral 2 y 3) determinan que nadie será objeto de injerencia arbitraria o ilegal en su vida privada. La Constitución del Ecuador (artículo 66, numerales 3, 19, 20) garantizan el derecho a la integridad personal, la protección de datos de carácter personal y el derecho a la intimidad personal y familiar. El 12 de julio de 2016 se presentó a la Asamblea Nacional un Proyecto de Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales (Proyecto número 254848). Sin embargo, este proyecto fue archivado. El 19 de septiembre de 2019, el Presidente presentó el Proyecto de Ley Orgánica de la Protección de Datos Personales (Proyecto número 379637).

Ahora bien, jurídicamente, la protección de datos personales surge como un mecanismo para salvaguardar el derecho a la intimidad de las personas. En términos generales, al hablar de datos personales nos referimos a cualquier información con respecto a una persona identificada o identificable, directa o indirectamente. La identificación directa requiere detalles básicos como el nombre, la edad, la dirección, el número de documento de identidad, un distintivo biométrico como el reconocimiento del iris o la huella digital, etc. La identificación indirecta requiere de otras características únicas o se da por una combinación de ellas, las cuales proporcionan suficiente información de identificación de una persona. Una persona identificable es aquella sobre la cual no se conoce su registro de identidad, pero puede llegar a ser determinado (Enríquez 2017).

En síntesis, el problema central de estas aplicaciones yace entonces en la falta de transparencia y certezas sobre la gestión, seguridad y posibles usos que se den a los datos que recopilan. Esta falta de claridad pone en riesgo la privacidad de los usuarios y, por ende, los coloca en una posición de indefensión frente a poderes públicos o privados que puedan servirse de esta información. En efecto, poco o nada se ha discutido en el país sobre la importancia del anonimato de los datos personales, biomédicos y de geolocalización que son compartidos por los ciudadanos en estas u otras aplicaciones. Tampoco se ha discutido sobre los riesgos que su irrespeto implica para la vida privada y el ejercicio de los derechos civiles y políticos. Esta falta de conciencia colectiva sobre el tema se refleja en la ausencia de un marco legal sobre la privacidad y la protección de datos. Sin dicho marco, la entrega, la recolección, el almacenamiento, procesamiento, divulgación, intercambio y comercialización de datos en el Ecuador se realiza, hoy por hoy, sin ninguna regulación.

Como en los albores del capitalismo, nos encontramos en un nuevo proceso de acumulación primaria, ya no de tierras o de recursos naturales, sino de datos e información basada en la anomia o la ley del más fuerte, que determinará la nueva estructura y trayectoria de las clases sociales y las relaciones internacionales. Si no hacemos algo urgente por actualizar nuestros marcos regulatorios nos encontraremos otra vez en el campo de los explotados. En efecto, la creación de estas bases de datos con información tan sensible, en contextos con poca o ninguna regulación, pueden dar lugar fácilmente al desarrollo de herramientas de vigilancia o sometimiento de los ciudadanos a intereses privados o del gobierno de turno. Un ejemplo que ilustra claramente estos riesgos es la posibilidad de que estas bases de datos se comercialicen o se filtren a terceros (aseguradoras privadas de salud, empleadores para evaluar a solicitantes de trabajo, partidos políticos, etc.), de forma intencionada o por accidente, y que esto determine el acceso o la cobertura que un ciudadano puede tener en el sistema de salud local, las posibilidades de obtener un empleo o el ejercicio de sus derechos civiles y políticos.

No podemos dejar que el optimismo tecnológico, el oropel de los *smartphones* y otros artefactos, conviertan estas aplicaciones en falsos ejes de la gestión de la pandemia. Estas no pueden reemplazar otras prioridades como mejorar la capacidad de atención y el acceso al sistema de salud nacional, las pruebas y precauciones con la higiene y cuidado personal, que han demostrado su efectividad en frenar la curva de contagio de la epidemia.

Hacia una nueva arquitectura global de poder

El problema más inquietante del uso y despliegue de estas tecnologías de monitoreo y control que ponen en riesgo dere-

chos, como la privacidad, son sus efectos de mediano y largo plazo sobre la estructura de poder y los sistemas democráticos. Como nos muestra la historia, la evolución de las epidemias y las estructuras del Estado están íntimamente relacionadas. En ese sentido, la pertinencia de estas nuevas tecnologías y dispositivos no debe evaluarse únicamente mirando su capacidad para controlar la crisis actual, sino también sus consecuencias futuras y a las transformaciones que introducirán en la estructura y el funcionamiento de los mismos Estados. ¿Qué de toda esta panoplia de dispositivos, tecnologías y políticas que se nos ha impuesto durante esta crisis, será conservada por los gobiernos o las empresas luego de esta crisis para incrementar su poder y mejorar el control sobre las poblaciones? ¿Qué ocurre cuando la cesión de nuestra privacidad es enmarcada como un asunto de salud pública y no de control y poder?

Algunos eventos y políticas puestas en marcha en diferentes lugares del mundo en apenas seis meses dan la pauta del tipo de sistema político y económico al que puede conducirnos la implementación indiscriminada, apresurada y sin control democrático de estos dispositivos. En Colombia, por ejemplo, las medidas de control de la pandemia se están convirtiendo en auténticos sistemas de vigilancia y discriminación. Según un reporte de Índice Coronavirus y Derechos Digitales (2020), tanto instituciones públicas como empresas privadas están empezando a obligar a sus empleados a dar una serie de informaciones personales como preexistencias en salud, embarazos, VIH, desplazamientos, viajes, contactos, accidentes de tránsito, etc., que no guardan ninguna relación con la pandemia. La recolección de estos datos a través de formularios compartidos con poca o ninguna seguridad responde a las políticas implementadas por el gobierno para la reapertura y reactivación de la economía. En efecto, en su afán de precautelar la salud de los trabajadores el gobierno exige a las ins-

tituciones y empresas que desarrollen protocolos e informes sobre la salud y la seguridad de sus empleados. Estas, para poder retomar sus actividades, implementan apresuradamente dispositivos como los mencionados, muchas a través de aplicaciones, formularios inseguros o empresas tercerizadoras. Los empleados, por su parte, están obligados a llenar dichos formularios so pena de sanciones o despido. De hecho, incluso las personas que trabajan en línea están obligadas a llenar los formularios para poder seguir laborando. De esta manera, una política que en principio estaba orientada a proteger a los trabajadores, termina generando más riesgo y convirtiéndose en instrumento de discriminación o restricción de derechos para sus supuestos beneficiarios.

El problema radica en que, en ausencia de regulaciones claras sobre la protección de datos y la privacidad, este tipo de dispositivos y políticas puestos en marcha por los Estados terminan convirtiéndolos en una suerte de 'virus institucional' que replica lógicas de vigilancia y control en cada poro del tejido social. Es precisamente lo que devela el caso colombiano o ecuatoriano. El Estado emite políticas o normativas generales que las empresas y los ciudadanos están obligados a cumplir, pero no se especifican marcos y límites claros a las acciones demandadas, marcos que deberían ser definidos democráticamente. En ausencia de directrices claras, las empresas y los ciudadanos no tienen otra referencia que las acciones del mismo gobierno que, con el despliegue y uso indiscriminado que da a estos dispositivos y tecnologías, envía una fuerte señal de la poca importancia que se debe dar a la privacidad. Así, ya sea por obligación tácita o implícita, se comienza a construir una 'nueva normalidad' en la que cámaras, drones, captores biométricos, aplicaciones y demás terminan volviéndose parte del paisaje cotidiano y nuestros derechos y sentido de privacidad y libertad, una reliquia del siglo pasado.

En contextos autoritarios, las consecuencias políticas del despliegue de estas tecnologías de control pueden ser aún más evidentes. En Qatar, por ejemplo, la aplicación de *contact tracing* Ehteraz usa un sistema centralizado basado en tecnología Bluetooth y GPS para identificar posibles exposiciones a personas infectadas con COVID-19. Esta aplicación se volvió obligatoria en mayo con una pena de prisión de hasta 3 años para toda persona que no la haya descargado (Hern 2020). Los riesgos de sistema centralizado de localización y trazado de contactos con obligatoriedad de uso so pena de prisión en una monarquía absoluta pueden ser enormes para sus habitantes.

Finalmente, para entender las transformaciones políticas que este tipo de tecnologías están produciendo probablemente el mejor lugar para observarlas sean los mismos países asiáticos donde todo esto empezó. El caso de la ciudad de Hangzhou, en China, es un ejemplo paradigmático. Esta metrópoli de casi 10 millones de habitantes ubicada al sur de Shanghai y a unos 700 km de Wuhan —epicentro de la pandemia— es la cuna de Alibaba, la empresa digital más importante de China, y de la aplicación AliPay Health Code, desarrollada por la misma empresa. Luego de haberse implementado a nivel nacional y una vez que la primera ola de contagio parece estar bajo control, las autoridades de dicha ciudad han decidido extender indefinidamente el uso de esta aplicación e integrarlo con más indicadores de salud individuales. Estos indicadores podrían incluir no solo datos médicos, sino también niveles de actividad, estilos de vida (deporte, consumo de alcohol o tabaco, horas de sueño, etc.). En esta nueva versión, el usuario ya no verá en su pantalla los tres colores utilizados para restringir la movilidad en la pandemia, sino una escala de colores indicando su estado de salud (Davidson 2020). Como en el caso colombiano, la intención declarada por las autoridades chinas es ayudar a mejorar la salud de sus ciudadanos. Sin

embargo, en un régimen autoritario que antes de la pandemia utilizaba ya un sistema de 'crédito social' (DW 2019; Louvet 2019) basado en la vigilancia absoluta de sus ciudadanos y con capacidad para restringir varios de sus derechos en función de su 'buen' comportamiento, es fácil imaginar que estos datos puedan ser usados para mantener un control aún mayor de su población a través de sistemas de disciplinamiento automatizados. Podrían, por ejemplo, hacer pagar más a una persona por acceder a servicios de salud si mantiene 'malos' hábitos o restringir su acceso a trabajos, lugares, transportes, servicios, etc. Son múltiples las posibilidades de realización de escenarios distópicos en una sociedad que ha perdido el sentido del valor de la privacidad.

Hasta hace solo seis meses, se podía haber pensado que las posibilidades de generalización de este tipo de modelos autoritarios de disciplinamiento automatizado de las poblaciones difícilmente podrían exportarse a democracias occidentales. Sin embargo, muchas de las piezas que componen dichos sistemas, como ciertas redes sociales, servicios de comunicación o los sistemas de videovigilancia y reconocimiento facial han sido ya adoptados en varios países. En Ecuador, por ejemplo, el sistema de seguridad ECU 911, que cuenta hoy en día con 4500 cámaras de vigilancia en todo el país, fue equipado con tecnología de empresas chinas en el marco de un acuerdo de cooperación durante el gobierno de Correa. El uso político que se ha dado a la tecnología de vigilancia con la que cuenta este sistema ha sido denunciada por varios activistas (Mozur, Kessel, y Chan 2019). No obstante, el alcalde de Quito anunció que dicho sistema contaba ahora además con sistemas de reconocimiento facial (Rodríguez 2019). Como señalan Mozur et al. (2019), la diferencia con los sistemas de vigilancia que existen en países occidentales es que la tecnología china es más barata y, sobre la base de acuerdos de cooperación y fi-

nanciamiento como los realizados con Ecuador, está cada vez más fácilmente al alcance de cualquier país. Estos sistemas y otros como el rastreo GPS o las aplicaciones móviles, como las Corona-Apps, están creando la infraestructura necesaria para la implantación de sistemas de disciplinamiento automatizado. Si a esto se suma el estado de excepción y la necesidad de reactivar la economía y recuperar la movilidad, las posibilidades de que se obligue a los ciudadanos a usar dispositivos de vigilancia y control como los analizados, con el pretexto de preservar la salud pública, no son menores.

A modo de conclusión: el omnióptico

Como hemos mencionado, la cuarentena global, de la cual el Ecuador es parte, revela una desarticulación del modelo panóptico de poder. Un retroceso en la capacidad de los Estados para mantener la disciplina y el orden entre sus poblaciones. Sin embargo, el aparecimiento de nuevos métodos y dispositivos de control sugiere que este retroceso en el modelo disciplinario moderno no es más que un repliegue táctico. En realidad, estamos presenciando el surgimiento de una nueva arquitectura de poder a escala global: el omnióptico. Este modelo ofrece las mismas ventajas disciplinarias del diseño de Bentham pero con la elegancia de la Biblioteca de Babel de Borges. Diseñada en un espacio virtual, esta arquitectura crea un mundo donde todos pueden ser vistos, escuchados, localizados, medidos, comprendidos y pronosticados sin necesidad de torres, muros, ventanas o perros guardianes. Como en el modelo panóptico, no importa quién nos vigile, o incluso si hay alguien que realmente nos observa: la disciplina se interioriza por el miedo.

Sin embargo, se pueden identificar dos grandes diferencias. En primer lugar, este nuevo modelo no se limita a la existencia

real de instituciones o espacios físicos que disciplinen a los individuos (escuelas, prisiones, hospitales, etc.). Este está diluido a nuestro alrededor, lo construimos cada día con nuestros rastros digitales, nuestros movimientos físicos, nuestros parpadeos y nuestros latidos. Puede estar en cualquier lugar y en cualquier momento. Por lo tanto, no puede ser contenido ni dirigido por entidades limitadas como los Estados modernos. Nos enfrentamos al surgimiento de una estructura global de poder sin una entidad política capaz de controlarla. En segundo lugar, en el modelo bethamiano, el puesto del vigilante podía ser ocupado por cualquier individuo y, por lo tanto, cualquier persona fuera del panóptico podría supervisar lo que hace dicho vigilante. Había una cierta forma de transparencia y control sobre quienes ejercen el control para evitar que el modelo se convierta en una tiranía. Sin embargo, en el nuevo omnióptico, esta característica de transparencia y rendición de cuentas se desvanece en la automatización producida por las tecnologías de Big Data y la inteligencia artificial. De hecho, en esta nueva arquitectura no solo los cuerpos físicos, sino también los pensamientos, deseos, sentimientos y la forma en que se manifiestan física y biológicamente se pueden ver, recolectar, analizar, explotar, predecir e instrumentalizar para disciplinar y controlar a la población. Sin embargo, ningún ser humano puede ocupar la posición del vigilante (una vida entera no sería suficiente para ver, oír y analizar toda la información que estos dispositivos recolectan en un solo día) ni puede supervisar algo que no entiende (los algoritmos que ocupan hoy en día el puesto del vigilante no son producidos por humanos sino por otros algoritmos). Como en las cuarentenas del siglo XVII, este nuevo modelo disciplinario que se está apoderando de los Estados modernos del mundo, nos encerrará a todos nosotros (incluidos los vigilantes) en nuestras celdas, dejará las llaves fuera de las puertas y a nadie del otro lado para que las abra cuando la crisis se acabe.

Bibliografía

Abrams, Lawrence. 2020. "Over 500,000 Zoom accounts sold on hacker forums, the dark web". *Bleeping Computer* (blog). 13 de abril de 2020. Disponible en: https://www.bleepingcomputer.com/news/security/over-500-000-zoom-accounts-sold-on-hacker-forums-the-dark-web/.

Amer, Karim. 2019. *The Great Hack*. Netflix. Disponible en: https://www.netflix.com/ec-en/title/80117542.

Bakkemo, Peter. 2020. "COVID-19 in the Arctic: Dramatic Increase at Russian Construction Site, Introduces Ankle Bracelets to Prevent Spreading". *High North News*, 27 de abril de 2020. Disponible en: https://www.highnorthnews.com/en/COVID-19-arctic-dramatic-increase-russian-construction-site-introduces-ankle-bracelets-prevent.

Bayer, Ronald, y Amy Fairchild. 2002. "The Limits of Privacy: Surveillance and the Control of Disease". *Health care analysis : HCA* 10 (febrero): 19-35. Disponible en: https://doi.org/10.1023/A:1015698411824.

Beauvieux, Fleur. 2012. "Épidémie, pouvoir municipal et transformation de l'espace urbain : la peste de 1720-1722 à Marseille". *Rives méditerranéennes*, n.º 42 (junio): 29-50. Disponible en: https://doi.org/10.4000/rives.4177.

Bentham, Jeremy. 1995. *Jeremy Bentham: The Panopticon Writings*. Editado por Miran Bozovic. London: Verso.

Bischoff, Paul. 2019. "Report: 267 Million Phone Numbers & Facebook User IDs Exposed Online". *Comparitech* (blog). 19 de diciembre de 2019. Disponible en: https://www.comparitech.com/blog/information-security/267-million-phone-numbers-exposed-online/.

Blickle, Kristian. 2020. "Pandemics Change Cities: Municipal Spending and Voter Extremism in Germany, 1918-1933". *SSRN*

Electronic Journal. Disponible en: https://doi.org/10.2139/ssrn.3592888.

Bouron, Françoise. 2009. "La grippe espagnole (1918-1919) dans les journaux français". *Guerres mondiales et conflits contemporains* n° 233 (1): 83-91.

Busvine, Douglas. 2020. "European Experts Ready Smartphone Technology to Help Stop Coronavirus". *Reuters*, 1 de abril de 2020. Disponible en: https://www.reuters.com/article/us-health-coronavirus-europe-tech-idUSKBN21J4HI.

Cadena, Santiago. 2019. "¿Está preparado el Ecuador para una fuga de datos masivos?". *EcuadorToday* (blog). 10 de octubre de 2019. Disponible en: https://ecuadortoday.media/2019/10/09/esta-preparado-el-ecuador-para-un-fuga-de-datos-masivos/.

Carvajal, Ana María. 2020. "Secretario de Seguridad del Municipio de Quito dejó su cargo". *El Comercio*, 23 de marzo de 2020. Disponible en: https://www.elcomercio.com/actualidad/secretario-seguridad-municipio-quito-renuncia.html.

Castañeda, Juan Diego, y Amalia Toledo. 2020. "El espejismo de las "coronapps": lecciones digitales para tiempos de emergencia". *El Espectador*, 21 de mayo de 2020. Disponible en: https://www.elespectador.com/coronavirus/el-espejismo-de-las-coronapps-lecciones-digitales-para-tiempos-de-emergencia-articulo-920463.

Chavez, Henry. 2017. "'Dreaming of electric sheep'. Les cycles techno-économiques du système mondial et le développement technoscientifique en Équateur : sources et limites du projet postnéolibéral (2007–2016)". Thèse de doctorat, Paris: EHESS.

Chávez, Henry, y Jacqueline Gaybor. 2018. "Science and Technology Internationalization and the Emergence of Peripheral Techno-Dreams: The Yachay Project Case". *Tapuya: Latin American Science, Technology and Society* 1 (1): 1-18. Disponible en: https://doi.org/10.1080/25729861.2018.1523522.

Cifuentes, Gonzalo. 2018. "Fondo estadounidense compra negocio de las huellas digitales en salud". *BioBioChile*, 3 de enero de 2018. Disponible en: http://www.biobiochile.cl/noticias/economia/negocios-y-empresas/2018/01/03/fondo-estadounidense-compra-negocio-de-las-huellas-digitales-en-salud.shtml.

Cimpanu, Catalin. 2019. "Adobe Left 7.5 Million Creative Cloud User Records Exposed Online". *ZDNet* (blog). 26 de octubre de 2019. Disponible en: https://www.zdnet.com/article/adobe-left-7-5-million-creative-cloud-user-records-exposed-online/.

Cole, Brendan. 2020. "Man Fined $33,000 after Breaking Coronavirus Quarantine to Go Partying at Nightclub in Taiwan". *Newsweek*, 23 de marzo de 2020. Disponible en: https://www.newsweek.com/taiwan-coronavirus-fine-taipei-quarantine-lockdown-COVID-19-1493726.

Cortes, Diego. 2019. "Nueva fuga de información del Servicio Electoral Chileno, cerca de 14 millones de chilenos afectados". *Seguridad y Firewall* (blog). 1 de agosto de 2019. Disponible en: http://www.seguridadyfirewall.cl/2019/08/nueva-fuga-de-informacion-del-servicio.html.

Davidson, Helen. 2020. "Chinese City Plans to Turn Coronavirus App into Permanent Health Tracker". *The Guardian*, 26 de mayo de 2020. Disponible en: https://www.theguardian.com/world/2020/may/26/chinese-city-plans-to-turn-coronavirus-app-into-permanent-health-tracker.

Diomedi P., Alexis. 2003. "La guerra biológica en la conquista del nuevo mundo: Una revisión histórica y sistemática de la literatura". *Revista chilena de infectología* 20 (1): 19-25. Disponible en: https://doi.org/10.4067/S0716-10182003000100003.

DW. 2019. *China: La vigilancia absoluta*. DW Documental. Disponible en: https://www.youtube.com/watch?v=S-q7_5M8Fxk.

El Colombiano. 2016. "La filtración de datos que afectó a millones de usuarios de LinkedIn". *El Colombiano*, 25 de mayo de 2016.

Disponible en: https://www.elcolombiano.com/tecnologia/la-filtracion-de-datos-que-afecto-a-millones-de-usuarios-de-linkedin-BF4214517.

Enríquez, Luis. 2017. "Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales". *Foro. Revista de Derecho*, n.º 27: 43-61.

Escande, Philippe. 2020. "L'application StopCovid est disponible au téléchargement sur iPhone et Android". *Le Monde*, 2 de junio de 2020.

Fairchild, Amy L., James Colgrove, y Ronald Bayer. 2003. "The Myth of Exceptionalism: The History of Venereal Disease Reporting in the Twentieth Century": *The Journal of Law, Medicine & Ethics*, diciembre. Disponible en: https://journals.sagepub.com/doi/10.1111/j.1748-720X.2003.tb00130.x.

Fernandes, Aaron. 2020. "Electronic Tracking Devices among New Coronavirus Powers for WA Security Agencies". *SBS News*, 11 de abril de 2020. Disponible en: https://www.sbs.com.au/news/electronic-tracking-devices-among-new-coronavirus-powers-for-wa-security-agencies.

Ferretti, Luca, Chris Wymant, Michelle Kendall, Lele Zhao, Anel Nurtay, Lucie Abeler-Dörner, Michael Parker, David Bonsall, y Christophe Fraser. 2020. "Quantifying SARS-CoV-2 Transmission Suggests Epidemic Control with Digital Contact Tracing". *Science* 368 (6491). Disponible en: https://doi.org/10.1126/science.abb6936.

FM Mundo. 2020. "Andrés Michelena, Aplicación Digital Para El COVID - 19". Web. *NotiMundo*. Quito: SoundCloud. Disponible en: https://soundcloud.com/mascomunicacion-1/notimundo-andres-michelena-aplicacion-digital-para-el-COVID-19.

Foucault, Michel. 1975. *Surveiller et punir: Naissance de la prison*. Paris: Gallimard.

———. 2004. *Naissance de la biopolitique: cours au Collège de France, 1978-1979*. Editado por François Ewald, Alessandro Fontana, y Michel Senellart. Hautes études. Paris: Gallimard : Seuil.

———. 2007. *Security, Territory, Population: Lectures at the College de France, 1977-78*. London: Palgrave Macmillan. Disponible en: http://www.azioni.nl/platform/wp-content/uploads/2013/04/Foucault-Security-Territory-Population.pdf.

Galvan, Menta. 2019. "5 grandes casos de fuga de datos y cómo pudieron evitarse". *Menta* (blog). 22 de julio de 2019. Disponible en: https://www.menta.com.mx/blog/post/5-grandes-casos-de-fuga-de-datos-y-como-pudieron-evitarse.

Gebhart, Gennie, y Bennett Cyphers. 2020. "Governments Shouldn't Use 'Centralized' Proximity Tracking Technology". *Electronic Frontier Foundation* (blog). 12 de mayo de 2020. Disponible en: https://www.eff.org/deeplinks/2020/05/governments-shouldnt-use-centralized-proximity-tracking-technology.

Girard, Laurence. 2020. "Coronavirus : Apple et Google proposent un outil commun pour les applications de traçage des malades". *Le Monde*, 10 de abril de 2020. Disponible en: https://www.lemonde.fr/pixels/article/2020/04/10/coronavirus-apple-et-google-proposent-un-outil-commun-pour-les-applications-de-tracage-des-malades_6036278_4408996.html.

Hautala, Laura. 2020. "Filtración en Perú expuso información de clientes de una cadena de cines". *CNET en español*, 27 de enero de 2020. Disponible en: https://www.cnet.com/es/noticias/peru-fuga-datos-cineplanet/.

Heran, Juan. 2018. "México: datos personales de más de 2 millones de pacientes expuestos en Internet". *WeLiveSecurity*, 7 de agosto de 2018. Disponible en: https://www.welivesecurity.com/la-es/2018/08/07/datos-personales-pacientes-mexico-expuestos-internet/.

Hern, Alex. 2020. "Qatari Contact-Tracing App 'Put 1m People's Sensitive Data at Risk'". *The Guardian*, 27 de mayo de 2020. Disponible en: https://www.theguardian.com/world/2020/may/27/qatar-contact-tracing-app-1m-people-sensitive-data-at-risk-coronavirus-COVID-19.

Hildesheimer, Françoise. 1993. *Fléaux et Société : De La Grande Peste Au Choléra, XIVe-XIXe Siècle*. Paris: Hachette Livre. Disponible en: https://gallica.bnf.fr/ark:/12148/bpt6k48133051.

Hootsuite, y We are social. 2020. "Digital 2020: Ecuador". Disponible en: https://datareportal.com.

Índice coronavirus, y Derechos Digitales. 2020. "El jefe es el Gran Hermano: trabajo o privacidad". *Índice* (blog). 4 de junio de 2020. /post2/.

Infobae. 2020. "'Cuídate en casa', una aplicación para controlar el cumplimiento de la cuarentena". *Infobae*, 30 de marzo de 2020. Disponible en: https://www.infobae.com/tecno/2020/03/30/cuidate-en-casa-una-aplicacion-para-controlar-el-cumplimiento-de-la-cuarentena/.

Jasanoff, Sheila, y Sang-Hyun Kim, eds. 2015. *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power*. 1.ª ed. Chicago; London: University of Chicago Press. Disponible en: https://b-ok.cc/book/2610333/642648.

Jee, Charlotte. 2019. "Facebook Has Leaked 419 Million Phone Numbers". *MIT Technology Review* (blog). 5 de septiembre de 2019. Disponible en: https://www.technologyreview.com/2019/09/05/133154/facebook-has-leaked-419-million-phone-numbers/.

Kim, Max S. 2020. "South Korea Is Watching Quarantined Citizens with a Smartphone App". *MIT Technology Review* (blog). 6 de marzo de 2020. Disponible en: https://www.technologyreview.com/2020/03/06/905459/coronavirus-south-korea-smartphone-app-quarantine/.

Kobeissi, Nadim. 2020. "Why StopCOVID Fails as a Privacy-Preserving Design". *Nadim Kobeissi* (blog). 27 de mayo de 2020.

Disponible en: https://nadim.computer/posts/2020-05-27-stopcovid.html.

Lapowsky, Issie. 2018. "Facebook Exposed 87 Million Users to Cambridge Analytica". *Wired*, 4 de abril de 2018. Disponible en: https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/.

———. 2019. "How Cambridge Analytica Sparked the Great Privacy Awakening". *Wired*, 17 de marzo de 2019. Disponible en: https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/.

Latour, Bruno. 2001. *Les microbes guerre et paix des microbes*. Paris: La Découverte.

Louvet, Sylvain. 2019. *Tous surveillés: 7 milliards de suspects*. Documental. Arte. Disponible en: https://www.youtube.com/watch?v=Hf1JR0HP4rM.

Lyons, Kim. 2020. "Germany Says Its Coronavirus Contact Tracing App Is Ready". *The Verge* (blog). 14 de junio de 2020. Disponible en: https://www.theverge.com/2020/6/14/21290874/germany-contact-tracing-coronavirus.

McCormick, Rich. 2014. "Hack Leaks Hundreds of Nude Celebrity Photos". *The Verge* (blog). 1 de septiembre de 2014. Disponible en: https://www.theverge.com/2014/9/1/6092089/nude-celebrity-hack.

Miller, Joe, y Guy Chazan. 2020. "Contact-Tracing Apps Raise Privacy Concerns in Germany". *Financial Times*, 16 de abril de 2020. Disponible en: https://www.ft.com/content/32b6a360-3e22-47a3-ace5-60f42cc6b42d.

Mozur, Paul, Jonah Kessel, y Melissa Chan. 2019. "Hecho en China y exportado a Ecuador: el aparato de vigilancia estatal". *The New York Times*, 24 de abril de 2019. Disponible en: https://www.nytimes.com/es/2019/04/24/espanol/america-latina/ecuador-vigilancia-seguridad-china.html.

Mozur, Paul, Raymond Zhong, y Aaron Krolik. 2020. "In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags".

The New York Times, 1 de marzo de 2020. Disponible en: https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html.

Musil, Steven. 2019. "Wyze admite haber dejado expuestos los datos de millones de usuarios". *CNET en español*, 30 de diciembre de 2019. Disponible en: https://www.cnet.com/es/noticias/wyze-brecha-datos-millones-de-usuarios-expuestos/.

Myers, Julie, Thomas Frieden, Kamal Bherwani, y Kelly Henning. 2008. "Ethics in Public Health Research". *American Journal of Public Health* 98 (5): 793-801. Disponible en: https://doi.org/10.2105/AJPH.2006.107706.

Nikel, David. 2020. "Norway: 1.4 Million People Download Coronavirus Tracking App Despite Security Concerns". *Forbes*, 25 de abril de 2020. Disponible en: https://www.forbes.com/sites/davidnikel/2020/04/25/norway-14-million-people-download-coronavirus-tracking-app-despite-security-concerns/#753c293c7832.

Nunn, Nathan. 2010. "The Columbian Exchange: A History of Disease, Food, and Ideas". *The Journal of Economic Perspectives* 24 (2): 163-88.

PEPP-PT. 2020. "Pan-European Privacy-Preserving Proximity Tracing". Pepp Pt. 14 de junio de 2020. Disponible en: https://www.pepp-pt.org.

PlanV. 2019. "La peor filtración de datos en la historia del Ecuador al descubierto". *Plan V*, 16 de septiembre de 2019. https://www.planv.com.ec/historias/sociedad/la-peor-filtracion-datos-la-historia-del-ecuador-al-descubierto.

Quétel, Claude. 1984. "Syphilis et politiques de santé à l'époque moderne". *Histoire, économie & société* 3 (4): 543-56. Disponible en: https://doi.org/10.3406/hes.1984.1374.

Rodríguez, Valentina. 2019. "Reconocimiento facial en el límite entre la seguridad y la pérdida de privacidad". *Primicias* (blog). 24 de junio de 2019. Disponible en: https://www.primicias.ec/

noticias/tecnologia/reconocimiento-facial-seguridad-privacidad/.

Sallmann, Jean-Michel. 2011. *Le grand désenclavement du monde*. Paris: Payot.

Sardon, Jean-Paul. 2020. "De la longue histoire des épidémies au COVID-19". *Les analyses de Population Avenir* N° 26 (5): 1-18.

Satter, Raphael. 2020. "To Keep COVID-19 Patients Home, Some U.S. States Weigh House Arrest Tech". *Reuters*, 7 de mayo de 2020. Disponible en: https://www.reuters.com/article/us-health-coronavirus-quarantine-tech-idUSKBN22J1U8.

Sputnik. 2020. "Gobierno de Brasil lanza app para distribuir partida asistencial a trabajadores informales". *Sputnik*, 7 de abril de 2020. Disponible en: https://mundo.sputniknews.com/america-latina/202004071091041224-gobierno-de-brasil-lanza-app-para-distribuir-partida-asistencial-a-trabajadores-informales/.

Stivers, Richard, y Peter Stirk. 2001. *Technology as Magic: The Triumph of the Irrational*. Edición: Reprint. New York: Continnuum-3PL.

Suazo, Camilo. 2020. "Aplicaciones falsas de rastreo del coronavirus buscan robar datos personales". *BioBioChile*, 10 de junio de 2020. Disponible en: https://www.biobiochile.cl/noticias/ciencia-y-tecnologia/pc-e-internet/2020/06/10/aplicaciones-falsas-rastreo-del-coronavirus-buscan-robar-datos-personales.shtml.

Teleamazonas. 2020. *Andrés Michelena, ministro de Telecomunicaciones, comenta sobre la aplicación 'CovidEC'*. Quito: YouTube. Disponible en: https://www.youtube.com/watch?v=jGney-MuuOCg.

Untersinger, Martin. 2020a. "Contre le coronavirus, les immenses défis et les inconnues des applications mobiles de 'suivi de contacts'". *Le Monde*, 15 de abril de 2020. Disponible en: https://www.lemonde.fr/pixels/article/2020/04/15/contre-le-COVID-19-les-immenses-defis-et-inconnues-des-applica-

tions-mobiles-de-suivi-de-contacts_6036704_4408996.html.

———. 2020b. "StopCovid, une application de traçage passée en deux mois de l'idée dystopique à l'Assemblée". *Le Monde*, 27 de abril de 2020. Disponible en: https://www.lemonde.fr/pixels/article/2020/04/27/stopcovid-une-application-de-tracage-passee-en-deux-mois-de-l-idee-dystopique-a-l-assemblee_6037924_4408996.html.

Untersinger, Martin, y Pierre Breteau. 2020. "Faut-il ou non installer 'StopCovid'? Le débat résumé en une conversation SMS". *Le Monde*, 1 de junio de 2020. Disponible en: https://www.lemonde.fr/les-decodeurs/article/2020/06/01/faut-il-ou-non-installer-stopcovid-le-debat-resume-en-discussion-sms_6041417_4355770.html.

Žižek, Slavoj. 2020. "Slavoj Žižek: 'el Coronavirus es un golpe a lo Kill Bill al sistema capitalista'". *Esferapública* (blog). 18 de marzo de 2020. Disponible en: http://esferapublica.org/nf-blog/slavoj-zizek-el-coronavirus-es-un-golpe-a-lo-kill-bill-al-sistema-capitalista/.