



# Aplicación de dispositivos digitales para vigilar, enfrentar y controlar la pandemia de COVID-19 en 2020

Application of Digital Devices to Monitor, Face and Control the COVID-19 Pandemic in 2020

Aplicació de dispositius digitals per a vigilar, enfrontar i controlar la pandèmia de COVID-19 en 2020

**Josué García Veiga** 

Universidad Nacional Autónoma de México  
josuegave@hotmail.com

**Lorena Sánchez Preciado** 

Universidad Nacional Autónoma de México  
lorenapreciado.sp@gmail.com

**Recibido:** 13/11/2021

**Aceptado:** 23/12/2021



**Resumen** Frente a la emergencia sanitaria detonada en diciembre de 2019 por la pandemia de COVID-19 la mayoría de los países en el mundo han implementado soluciones tecnológicas digitales para el resguardo de la salud pública. La presente investigación tiene como objetivo principal ubicar la instrumentalización de tecnologías digitales con fines de vigilar, controlar y administrar las situaciones que emergen bajo el contexto de crisis sanitaria provocada por el virus SARS-CoV-2. De esta manera la investigación presenta una sistematización de las tecnologías digitales a nivel mundial de acuerdo con sus principales aplicaciones de vigilar y controlar. El texto propone una lectura de la pandemia desde un enfoque biopolítico que retoma los aportes de Foucault y Deleuze para identificar una lógica planetaria en el empleo de tecnologías digitales como dispositivos de disciplinamiento y control social.

**Palabras clave** Cibercontrol, biopolítica, capitalismo de la vigilancia, pandemia, vigilancia.

**Abstract** Faced with the health emergency triggered by the COVID-19 pandemic in December 2019, most countries in the world have implemented digital technological solutions to protect public health. The main objective of this article is to identify the instrumentalization of digital technologies used to monitor, control and manage the situations that emerged in the context of the current health crisis caused by SARS-CoV-2. In this way, the research presents a systematization of digital technologies worldwide according to their main surveillance and control application. The text proposes an interpretation of the pandemic from a biopolitical approach that considers the contributions of Foucault and Deleuze to identify a planetary logic in the use of digital technologies as dispositives of disciplining and social control.

**Keywords** Cybercontrol, Biopolitics, Surveillance capitalisme, Pandemic, Surveillance.

**Resum** Enfront de l'emergència sanitària detonada al desembre de 2019 per la pandèmia de COVID-19 la majoria dels països en el món han implementat solucions tecnològiques digitals per al resguard de la salut pública. La present recerca té com a objectiu principal situar la instrumentalització de tecnologies digitals amb finalitats de vigilar, controlar i administrar les situacions que emergeixen sota el context de crisi sanitària provocada pel virus SARS-CoV-2. D'aquesta manera la recerca presenta una sistematització de les tecnologies digitals a nivell mundial d'acord amb les seves principals aplicacions de vigilar i controlar. El text proposa una lectura de la pandèmia des d'un enfocament biopolític que reprèn les aportacions de Foucault i Deleuze per a identificar una lògica planetària en l'ús de tecnologies digitals com a dispositius de disciplinament i control social.

**Paraules clau** Cibercontrol, biopolítica, capitalisme de la vigilància, pandèmia, vigilància.

\* Investigación realizada gracias al Programa UNAM-PAPIIT-IN303721 "Trayectorias del gran capital en México. Problemas económicos y ambientales 2012-2023" en el Observatorio Latinoamericano de Geopolítica del Instituto de Investigaciones Económicas, UNAM

## Introducción

Existe una premisa que afirma que en épocas de crisis es de vital importancia contar con información precisa, útil y actualizada. Con esta aseveración abre el “Compendio de iniciativas de gobierno digital en respuesta a la pandemia COVID-19” publicado por la Organización de Naciones Unidas (UN, 2020). La expresión se refiere a un *sentido común*: a mayor información, mejores serán las decisiones tomadas frente a la crisis sanitaria (Lim, 2020). De esta manera en nombre de la Salud Pública encontramos hoy en día la justificación para implementar tecnologías digitales con el objetivo de obtener en tiempo real la información más detallada del estado de la pandemia. El carácter de urgencia de la situación extraordinaria, hace que su implementación sea acelerada y en muchos casos abrupta, soslayando discusiones y escrutinios cuidadosos sobre las implicaciones del uso de estas tecnologías en un mayor número de actividades cotidianas.

En la discusión actual varios autores interpretan la reciente instrumentalización de tecnologías digitales y su papel en las lógicas de control, vigilancia y normalización. La nueva ola global de aplicaciones tecnológicas digitales a escala planetaria, por un lado actualiza en cierta medida los mecanismos de disciplinarios, pero al mismo tiempo desborda los límites de los tradicionales moldes del encierro, apuntando hacia nuevas formas abigarradas y flexibles, extendiendo las prácticas de control y la vigilancia sobre nuevos ámbitos de manera a veces más sutiles, normalizadas e incluso aceptadas por vastos sectores de la población (ej. el portar celulares inteligentes y las aplicaciones de rastreo). Se trata de un proceso biopolítico a nivel mundial descentralizado y con el involucramiento de diversas tecnologías, discursos, instituciones y sujetos con distintos alcances y escalas bajo imperativos y fines comunes: vigilar, modificar o conservar el comportamiento de la población para garantizar el orden del ejercicio del poder y la acumulación capitalista. La presente investigación tiene como propósito central ubicar la instrumentalización de tecnologías digitales orientadas a las prácticas de vigilar y controlar que surgen bajo el contexto bélico contra la pandemia COVID-19.

En la primera parte del texto se hace una breve revisión de los aportes de Michel Foucault al estudio de los dispositivos y mecanismos de poder; junto con los posteriores desarrollos de Gilles Deleuze sobre las sociedades de control, y lo referente al desarrollo de la infraestructura totalizante cibernética explicado en el artículo *La hipótesis cibernética* (2013) de la revista *Tiqqun*. En la segunda parte se sistematizan los principales usos de las tecnologías digitales que emergen en el actual contexto de crisis sanitaria y que cumplen con funciones de vigilar y controlar a las distintas poblaciones del mundo. En la última sección se problematiza la “cibervigilancia” partiendo de varias interpretaciones contemporáneas sobre el despliegue de diversos dispositivos tecnológicos para controlar y enfrentar la pandemia.

## Marco Teórico

A continuación se exponen algunas de las nociones teóricas que explican el ejercicio del poder, control y la vigilancia en las sociedades contemporáneas. Esto con aras de reflexionar la instrumentalización de dispositivos de control y vigilancia digitales durante la pandemia COVID-19, que tienen como objetivo, no sólo contener y enfrentar la crisis, sino extender lógicas de vigilancia y control a las poblaciones del mundo.

Partimos de Michel Foucault y sus reflexiones sobre el poder. Para el pensador francés, el poder no se puede considerar como una sustancia, fluido o algo que emana de las cosas, se trata más bien de “un conjunto de mecanismos y procedimientos” (Foucault, 2006 [1978]) a los cuales Foucault se pregunta cómo funciona y opera el poder. De ahí que los procedimientos sean las relaciones sociales “cuyo papel es establecer, mantener, transformar los mecanismos de poder” (2006:12).<sup>1</sup> Por su parte, el concepto de biopolítica pone de manifiesto el conjunto de mecanismos mediante los cuales se hace posible que los rasgos biológicos de la especie humana se vuelvan parte de una “estrategia general de poder” (Foucault, 2006 [1978]:15). Este punto de partida le permite a Foucault diferenciar entre mecanismos legales, disciplinarios y de seguridad. Para fines de este texto, nos centramos en los mecanismos disciplinarios y de seguridad.

Es necesario considerar que los distintos mecanismos de poder se ejercitan en tanto garantizan el mantenimiento de la seguridad, ya que se desdobra en “toda una serie de técnicas de vigilancia, vigilancia de los individuos, diagnóstico de lo que éstos son, clasificación de su estructura mental, patología propia, etc.” (Foucault, 2006 [1978]:23). Con esto, comprendemos que existe una correlación sistemática entre los mecanismos legales, disciplinarios y de seguridad lo que devendrá en una serie de técnicas de gubernamentalidad y de seguridad que combina, dentro de su propia lógica, elementos de los distintos tipos de mecanismos. En su clásico texto *Vigilar y Castigar* (2002 [1975]), Foucault analiza los mecanismos para gestionar la peste europea del siglo XVI y los enmarca como dispositivos disciplinarios en una situación de excepción. Las prácticas analizadas por Foucault describen la división tajante y el estricto control del espacio, una vigilancia apoyada en un registro centralizado de todos los cuerpos, la creación de jerarquías y otros esfuerzos para separar e individualizar a la población. Estos dispositivos de disciplinamiento social se

---

<sup>1</sup> De acuerdo con Edgardo Castro para pensar en el poder de forma reticular es necesario preguntarse: “a) qué sistemas de diferenciación permiten que unos actúen sobre otros (diferencias jurídicas, tradicionales, económicas, competencias cognitivas, etc.); b) qué objetivos se persiguen (mantener un privilegio, acumular riquezas, ejercer una profesión); c) qué modalidades instrumentales se utilizan (las palabras, el dinero, la vigilancia, los registros); d) qué formas de institucionalización están implicadas (las costumbres, las estructuras jurídicas, los reglamentos, las jerarquías, la burocracia); e) qué tipo de racionalidad está en juego (tecnológica, económica)” (Castro, 2004).

esparcieron sobre la población a lo largo de los siglos XVII, XVIII y XIX hasta llegar a su cénit con el panóptico de Bentham: un diagrama arquitectónico que logró materializar las relaciones de poder en un dispositivo físico espacial independiente de la persona que lo ejerce directamente, petrificando los efectos de la vigilancia con un funcionamiento continuo y a bajos costos. Posteriormente, la generalización del panoptismo normalizó la disciplina en un modelo funcional en toda la sociedad capitalista mediante dispositivos cada vez más sutiles que fueron interiorizados en procedimientos de control, encierro flexibles, transferibles y adaptables a varias instituciones como las fábricas, ejércitos, escuelas, cárceles, hospitales y policías civiles. De esta forma, los mecanismos disciplinarios, en conjunto con los mecanismos legales creadores de códigos aplicados a las poblaciones en general, presentan un pensamiento negativo (niegan: dicen lo que no se debe de hacer o no está permitido): “el orden, en efecto, es lo que queda una vez que se ha impedido todo lo que está prohibido”, (Foucault, 2006 [1978]). En suma, el mecanismo disciplinario en general hace una codificación de lo permitido y lo prohibido.

Por otra parte, Foucault diferencia a los mecanismo de seguridad de los anteriores al señalar que éstos no impiden o apuntan lo que es obligatorio, sino toman “la distancia suficiente para poder captar el punto donde las cosas van a producirse, sean deseables o indeseables” (Foucault, 2006 [1978]).<sup>2</sup> El mecanismo de seguridad funciona en tanto la ideología y técnica de gobierno liberal está presente: el liberalismo sostiene que las personas deben *laissez faire et laissez passer, le monde va de lui même*, lo que significa en última instancia, que la realidad deviene por sí sola y marcha siguiendo sus mecanismos y principios propios. De esta forma, el mecanismo de seguridad sólo puede funcionar para garantizar que todo se dé en libertad, entendida como las posibilidades de movimiento, desplazamiento y circulación de personas, así como de mercancías. El pensador francés también evidencia los mecanismos de seguridad utilizados durante la epidemia de viruela en Europa durante el siglo XVIII. Uno de ellos fue la vacunación, que permitió la doble integración de la “racionalización del azar y las probabilidades” del número de enfermos y contagios; este mecanismo de seguridad –la vacunación–, se volvió aceptable para los médicos y todos los encargados de la política médica. Esto dio paso a la normalización social

---

<sup>2</sup> En *Seguridad, territorio y población*, Foucault ilustra el funcionamiento de los mecanismos de seguridad con el concepto de escasez partiendo de las nociones fisiócratas sobre la libertad de circulación de los granos entendida como efecto lógico del sistema fisiocrático. Al respecto, el pensador francés menciona: “Me parece que podríamos mostrar con bastante facilidad que lo ocurrido entonces, y que motivó los grandes edictos o “declaraciones” de los años 1754-1764, fue en realidad, quizás a través y por obra del efecto multiplicador, el apoyo de los fisiócratas y su teoría, todo un cambio o, mejor dicho, una fase de un gran cambio en las técnicas de gobierno y uno de los elementos de la introducción de lo que llamaré dispositivos de seguridad. En otras palabras, el principio de la libre circulación de granos puede leerse como la consecuencia de un campo teórico, y al mismo tiempo como un episodio en la mutación de las tecnologías de poder y en el establecimiento de la técnica de los dispositivos de seguridad que a mi parecer es característica o es una de las características de las sociedades modernas” (Foucault, 2006 [1978]:51).

y extensión de la vacunación como mecanismo de seguridad con el fin de salvaguardar a las ciudades, –pensadas como centros de circulación y de contagio–, dando paso a una nueva técnica de poder moderna. En suma, con las concepciones foucaultianas comprendemos que los mecanismos disciplinarios, legales y de seguridad, son dispositivos de poder cuyo objeto son las poblaciones territorializadas para garantizar el mantenimiento del orden y reproducción del ejercicio de poder.

Otro filósofo francés que distingue las nuevas formas de control en las sociedades contemporáneas es Gilles Deleuze. A finales del siglo XX, Deleuze escribió el breve ensayo *Post Scriptum sobre las Sociedades de Control* (1999) donde especuló el desplazamiento de las sociedades de disciplinamiento por las “sociedades de control”. Ahí, Deleuze señala las nuevas implicaciones de las sociedades de control, que él concibe como “un nuevo monstruo”,<sup>3</sup> personificando la normalización progresiva y la instalación dispersa de un nuevo sistema de dominación. En el ensayo, Deleuze señala que los distintos moldes del encierro llegaron a su apogeo a inicios del siglo XX, pero entraron en crisis después de la segunda guerra mundial y pasaron a ser paulatinamente sustituidos por modulaciones<sup>4</sup> constantes de control. En las sociedades de control, dice Deleuze, “los controles constituyen una modulación, como una suerte de molde autodeformante que cambia constantemente y en cada instante, como un tamiz cuya malla varía en cada punto” (1999:5). A diferencia del maquinismo mecánico y analógico de las sociedades disciplinarias, los “controlatorios” constituyen un sistema de geometría variable cuyo lenguaje es numérico, que hoy podemos calificar como digital (que implica computadoras y otros dispositivos informáticos). Así, el control se realiza por medio de formas electrónicas de vigilancia en las sociedades de control. Deleuze identificó nuevos lugares de control y formas difusas de relaciones de poder que juegan un papel central en un entorno impulsado por la tecnología.

Este tipo de sociedad parte de un modelo de flujo que posibilita la acción a distancia sobre los individuos, quienes llevan consigo los datos que los identifican y controlan a través de la mediación de la tecnología (Lazzarato, 2006). Las sociedades de control están marcadas por un aumento cuantitativo y la normalización<sup>5</sup> de la vigilancia, habilitada por las tecnologías digitales de control. En consecuencia, el objetivo de las sociedades de control ya no es hacer que los cuerpos sean dóciles – como en las sociedades disciplinarias–, sino condicionar y moldear las percepciones

---

<sup>3</sup> Señala Deleuze: “Control es el nombre propuesto por Burroughs para designar al nuevo monstruo que Foucault reconoció como nuestro futuro inmediato” (1999: 5).

<sup>4</sup> Deleuze explica que los individuos en las sociedades de control se han fragmentado, al igual que la sociedad misma. En este contexto, el control se reinventa constantemente y asume diferentes formas, fragmentando así a los individuos.

<sup>5</sup> El enfoque de Deleuze sugiere que la comprensión del proceso de normalización de las sociedades de control implica considerar el contexto histórico, socioeconómico y tecnológico más amplio que condiciona la voluntad de las personas para aceptar tal tipo de sociedad y su (potencial) sistema asociado de dominación (Leclercq-Vandelannoitte y Aroles, 2020).

de los individuos, haciéndoles aceptar esta sociedad como normal (Leclercq-Vandellannoitte y Aroles, 2020).

Otro referente que inspira a la reflexión teórica sobre las nuevas técnicas de controlar y vigilar en su modalidad digital es el texto *La hipótesis cibernética* (2013) de la revista *Tiqqun*. Ahí, encontramos los elementos para comprender el auge de la cibernética<sup>6</sup> como una “nueva tecnología de gobierno que federa y asocia tanto la disciplina como la bio-política, tanto la policía como la publicidad, (...)” tanto el control como la normalización. La cibernética es así un “mundo autónomo de dispositivos confundidos con el proyecto capitalista en cuanto es un proyecto político” (Tiqqun, 2013). Es decir, la cibernética se ha vuelto una “máquina abstracta de guerra mundial” (Tiqqun, 2013). Con esto se pretende señalar que la cibernética tiene un efecto sobre los comportamientos físicos, biológicos y sociales: éstos son “programados y re-programables”. De esta manera la cibernética inaugura una serie de dispositivos, cuyo objetivo es tomar a su cargo o dirigir todo lo que existe. De ahí que *Tiqqun* la considere una técnica de gobierno que totaliza la sociedad. Esto afecta a las subjetividades y “produce totalidades colectivas”. En última instancia, con la cibernética se produce la idealización de una sociedad estabilizada que necesita de mecanismos socialmente controlables. La implantación de la totalización social debido a la cibernética no se puede comprender sin una serie de tecnologías digitales e innovaciones que la hacen posible, el internet es uno de ellos. Asimismo, la retroalimentación –entendida como circulación de información o *feedback*– es de total relevancia para la cibernética, en tanto la comunicación de un sistema entre sus partes permite el control. Esta perspectiva presentada por *Tiqqun*, contribuye a comprender el desarrollo del “capitalismo cibernético” que pone en el centro de su funcionamiento el pilotaje o control de los flujos de circulación.

A la luz de los referentes teóricos citados, interpretaremos la instrumentalización en curso de los diversos dispositivos de control y vigilancia digitales durante la pandemia de COVID-19.

## Metodología

Para estudiar las formas presentes en cómo se despliegan los mecanismos foucaultianos de disciplinamiento y seguridad junto con los deleuzianos de control, presentamos una sistematización de los principales usos tecnológicos digitales que emergen en el actual contexto de crisis sanitaria. El Cuadro 1 adapta la clasificación propuesta por Sera Whitelaw *et al.* (2020) publicada por la revista *Lancet Digital*

---

<sup>6</sup> Tiqqun retoma la etimología griega para dar sentido a la palabra cibernética: “El griego *kybernesis* significa, en sentido propio, “acción de pilotar una nave”, y, en sentido figurado, “acción de dirigir, de gobernar”.

*Health* la cuál nos sirve para ordenar las diferentes iniciativas tecnológicas digitales: rastreo de la pandemia, detección de infectados, seguimiento de posibles contagios, garantizar medidas de confinamiento y apoyar los diagnósticos clínicos. En cada una de ellas encontramos una hibridación de mecanismos, dispositivos foucaultianos y modulaciones deleuzianas, donde resulta limitado señalar las fronteras de estas categorías analíticas. En ellas observamos una combinación de tecnologías como la inteligencia artificial, el *big data* así como técnicas de localización, aplicaciones digitales, uso de drones y sensores u otro tipo de infraestructuras. No obstante la clasificación es funcional y práctica para sistematizar las tecnologías acordes a sus fines últimos: por ejemplo, existe una distinción entre los dispositivos para rastrear, localizar y mapear a las personas contagiadas, de aquellos mecanismos de confinamiento que prohíben la circulación de quienes resultaron positivo en las pruebas Sars-2.

La documentación de los casos está basada en una investigación de diversas fuentes periodísticas para el año 2020, adicionalmente retoma otros esfuerzos existentes por registrar estas tecnologías a nivel mundial como *COVID Tracing Tracker* realizado por MIT (2020); el informe especial de Freedom on The Net 2020 *The Pandemic's Digital Shadow* (Shahbaz y Funk, 2020); *COVID-19 Digital Rights Tracker* por TOP10VPN (Woodhams, 2021); la iniciativa *Pandemic Big Brother* (2020); el *Compendium of Digital Government Initiatives in response to the COVID-19 Pandemic* de Naciones Unidas (UN, 2020) y *Fighting the Global COVID -19 Power-Grab* de Privacy International.

## Resultados

### **Rastreo**

Desde el inicio de la pandemia de la COVID-19 en diciembre de 2019, los países emprendieron diversas estrategias y aplicaciones tecnológicas para rastrear el avance del virus al interior de su territorio. Existen usos de inteligencia artificial (IA) y de *big data* para mapear tanto la ubicación y el movimiento en tiempo real de las personas con el apoyo de teléfonos celulares, uso de redes sociales, aplicaciones digitales (*apps*, por su abreviatura en inglés, *programas* diseñados principalmente para dispositivos móviles), pagos con tarjetas u otras opciones tecnológicas diseñadas para rastrear (Whitelaw *et al.*, 2020).

Actualmente muchos países en el mundo están utilizando paneles de datos y mapas de calor como herramientas de información y medio gráfico para conocer y transmitir el estado de la pandemia. Son instrumentos que sirven para reorganizan la división social del espacio en la redefinición de los límites y el establecimiento de nuevas restricciones fronterizas como las zonas clasificadas de alto contagio. En

Argentina, la firma GranData publicó un mapa de calor diseñado para monitorear el cumplimiento de la cuarentena, basándose en datos de ubicación georreferenciada recopilados por otras *apps* digitales (PI, 2020). En este tipo de casos, la mayor parte de los usuarios desconocen el último paradero de su información y con qué fin son procesados. En casos como este los datos son obtenidos mediante la descarga de *apps* en los teléfonos móviles, necesarias para hacer el mapeo. En algunos países hemos visto como previo a la pandemia ya se contaba con programas de recopilación y sistematización de datos para ciertos fines “gubernamentales”, los cuales una vez iniciada la emergencia sanitaria, sólo tuvieron que modificar sus parámetros de búsqueda. Taiwán estableció un sistema de gestión de desastres (después del brote de SARS de 2003), que permitió una rápida respuesta tecnológica a la pandemia.

La lógica del rastreo o seguimiento tradicionalmente consiste en cualquier registro que sirva para generar identidades a cada uno de los pacientes de acuerdo con la observación monitoreada de su historial clínico realizado por el personal de salud, quienes adicionalmente brindan un servicio de atención médica con cierta periodicidad. La novedad durante la pandemia es la automatización de las labores de rastreo y seguimiento gracias a la popularidad de *apps* digitales en los teléfonos móviles de las personas; de esta manera el sector salud puede orientar el comportamiento de quienes estén en riesgo de contagio (Weidenslaufer *et al.*, 2020). Un ejemplo de los alcances lo proporciona la *app* EDUS de Costa Rica, que permite al personal de salud acceder al expediente médico de los pacientes en tiempo real, garantizando un análisis completo del historial médico de los pacientes y así determinar el tratamiento específico para sus problemas de salud. EDUS permite un monitoreo del paciente en las distintas fases de su atención médica para visualizar su evolución y determinar progresos; mientras que a los pacientes les facilita la revisión de medicamentos, agilizar su solicitud y reservar citas médicas en centros de salud cercanos o directamente en los hospitales (Solís, 2020).

En muchas ocasiones las *apps* de rastreo también son utilizadas para dar seguimiento no solo a los usuarios directos sino a sus contactos, de esta manera ubicar y dar seguimiento a los casos contagiados confirmados de SARS-CoV-2 se vuelve materia estratégica de Estado cuando se trata de detener la propagación del virus. En Rusia e Israel los datos de teléfonos y pagos con tarjetas de crédito son utilizados para el mapeo de contagios y así determinar quiénes deberán resguardarse en cuarentena por haber estado en contacto con un caso confirmado a una distancia menor de 2 metros y por un lapso mínimo de 10 minutos (Ilyushina, 2020).<sup>7</sup>

---

<sup>7</sup> La *app* llamada Tawakkalna (COVID-19 KSA) generada por el gobierno de Arabia Saudí difunde información sobre la cantidad de infectados; además sirve para proporcionar permisos de movimiento (para que los usuarios puedan salir al espacio público) y les notifica cuando se encuentran cerca de áreas con un elevado índice de contagio. La *app* Tawakkalna se complementa con otras: la *app* Teetammman que recopila datos de salud de personas en cuarentena, y la *app* Tabaud que rastrea contactos.

## ***Detección de infecciones***

Entre las medidas para combatir la pandemia se encuentra la vigilancia y el control del espacio público mediante dispositivos tecnológicos biométricos que sirven para examinar y buscar patrones de una persona contagiada o potencialmente contagiada entre los transeúntes. En este caso se trata de *apps* digitales móviles, algoritmos de reconocimiento facial y cámaras con sensores térmicos instaladas en sitios públicos altamente transitados que identifican algún síntoma de infección (como alta temperatura corporal) o miden la “sana” distancia entre los cuerpos. En Ecuador, el Servicio Integrado de Seguridad ECU911 implementó algoritmos de IA desarrollados por el Banco Interamericano de Desarrollo, llamado Distancia2, que sirve para medir la distancia entre personas y así evitar posibles contagios. La plataforma comprende un módulo de detección y análisis de imágenes en tiempo-real para actualizar de manera automática los indicadores de movimiento y mapas de calor (Riobo *et al.*, 2020).

En Estados Unidos el apoyo económico de la Ley CARES (Ley de Ayuda, Alivio y Seguridad Económica por Coronavirus, por sus siglas en inglés), promulgada el 27 de marzo de 2020, destinó 13.2 mil millones de dólares a la educación, de los cuales parte importante sirvió para adquirir dispositivos tecnológicos con cámaras térmicas y funciones de reconocimiento facial para usarse al interior de las escuelas (Barber 2020). En América Latina las cámaras térmicas son empleadas en el transporte público como es el caso de las líneas subterráneas de Panamá y México. En algunas ocasiones se equipan con algoritmos que corroboran el uso del cubrebocas, como se puede observar en el metro de París (Holmes *et al.*, 2020), o adaptar a dispositivos aéreos como los drones que utiliza la Policía metropolitana colombiana en coordinación con autoridades sanitarias (Almenara, 2020).

En Japón, a tan sólo a unos meses de que se lleven a cabo las Olimpiadas en Tokyo 2021, se planea equipar los espacios públicos como estadios y otros auditorios concurridos con sistemas de seguridad y vigilancia que cuenten con cámaras térmicas y de reconocimiento facial. Para lo cual se espera que el proveedor líder de tecnología sea la firma japonesa de autenticación biométrica NEC con sus algoritmos para escanear los rostros tanto de atletas, como de trabajadores, personal de prensa y público en general para identificar aquellas personas que han estado en contacto con otras personas contagiadas de SARS-CoV-2. El evento también contará con un equipo de robots para automatizar el uso de desinfectantes y aplicaciones de IA que estimen escenarios de congestión que puedan ser evitados (Burt, 2020).

## **Seguimiento de contactos**

El carácter digital de los dispositivos tecnológicos facilita las actividades de vigilancia en aquellos espacios y actividades considerados íntimos y privados. En el contexto de emergencia sanitaria se justifica extender la intromisión de los dispositivos de vigilancia más allá del espacio público: conocer ubicación geolocalizada, información sobre compras, lugares visitados, monitoreo de contactos, rasgos biométricos (patrones faciales, de voz, temperatura corporal, el ritmo cardíaco, entre otros). Por ejemplo, la *app* del gobierno alemán Corona-Datenspende recopila los signos vitales de personas voluntarias que usan relojes inteligentes o rastreadores de actividad física para determinar si son sintomáticos.

Los países asiáticos fueron los pioneros en la experimentación masiva de *apps* específicas destinadas al seguimiento de contactos. En Corea del Sur los primeros casos de COVID-19 se notificaron a finales de enero de 2020 y luego aumentaron semanas después. A medida que éstos crecían, las autoridades pusieron en marcha un mecanismo masivo de rastreo y prueba de contactos para identificar y luego aislar a las personas infectadas.

El uso de códigos QR (*Quick Response*), similares a los códigos de barras, también son aplicados para el seguimiento de contactos. Por ejemplo, en China los usuarios escanean códigos QR para compartir información sobre su estado de salud e historial de viajes, lo que sirve para rastrear si los usuarios han estado en contacto con personas infectadas. Este sistema fue desarrollado por el departamento de salud chino en conjunto con dos de sus gigantes de internet: Alibaba y Tencent (Gan y Culver, 2020). De esta manera se lleva un registro digital de las personas que coinciden en determinado lugar por cierto tiempo; y cuando una de esas personas es diagnosticada positivo, las autoridades pueden rastrear los lugares que visitó y quiénes estuvieron a su alrededor en los sitios donde están instalados los códigos QR para hacer levantamiento de datos. En distintas partes del mundo observamos aplicaciones similares. Un caso es la *app* ucraniana Diia que sirve para escanear códigos QR en lugares públicos y medios de transporte. Este sistema es similar al aplicado en Singapur, Australia y en la Ciudad de México.

Con el seguimiento de contactos los gobiernos y empresas buscan producir información útil sobre la COVID-19, rastrear el movimiento de las personas contagiadas, identificar aquellas expuestas e incluso dar un seguimiento al cumplimiento de las medidas de cuarentena (Cabrol *et al.*, 2020: 1). Existen varias formas para elaborar redes de contactos entre las que se destaca por su gran popularidad global el uso de *apps* digitales en dispositivos móviles. Al 27 de enero de 2021, se registraron 120 *apps* de seguimiento de contactos en 71 países (Woodhams, 2021). Para estas aplicaciones existen dos principales tipos de sistemas: a) centralizados y b) descentralizados. Con los sistemas centralizados, los datos de las personas son

almacenados en un servidor central administrado por la autoridad a cargo de la aplicación; mientras que en los sistemas descentralizados la información se almacena en el dispositivo móvil de los usuarios para luego ser compartida con la autoridad sanitaria.

Entre las técnicas de rastreo más comunes encontramos al *bluetooth* y GPS, aunque también son utilizadas las señales telefónicas, los códigos QR y las redes sociales digitales, entre otras. De las 120 *apps* registradas a enero de 2021, 25% usan GPS como método de rastreo principal, 48% *bluetooth*, 22% usan ambos y el restantes 5% implementan vías alternativas (Woodhams, 2021). El gobierno de Singapur promovió el uso e instalación de una *app* llamada TraceTogether, que intercambia señales *bluetooth* entre teléfonos móviles cercanos. Una *app* de teléfono móvil puede hacer que el rastreo de contactos y la respectiva notificación sean instantáneos tras la confirmación del caso de contagio.

Las *apps* que utilizan GPS localizan los contactos de una persona al rastrear los movimientos del teléfono y de esta manera ubicar otros teléfonos que permanecieron en la misma ubicación por cierto tiempo. El alcance de estas *apps* digitales muestra una gama muy amplia de combinaciones tecnológicas con usos específicos; prácticamente en todo el mundo se registran su uso. Los estados de la Unión Europea activaron *apps* nacionales para intercambiar información a través de las fronteras nacionales, de modo que los usuarios solo tenían que instalar una única *app* para saber si han estado en contacto con personas contagiadas en toda la Unión Europea. A diferencia de algunas *apps* asiáticas, las europeas que utilizan el *bluetooth*, se instalan voluntariamente y respetan la privacidad de los usuarios al no permitir el seguimiento de las ubicaciones de las personas (CE, 2020a).

En América Latina y el Caribe se identifican al menos 6 países (Brasil, Ecuador, Haití, México, Perú y República Dominicana) donde las *apps* digitales presentan opciones de seguimiento de contactos (Ceceña y García, 2021).

Por otra parte, Apple y Google lanzaron su interfaz privada de programación (API, por sus siglas en inglés) para colaborar en el rastreo de contactos. En mayo de 2020, ambas empresas presentaron su API: “Exposure Notifications API” que permite la interoperabilidad entre dispositivos iOS y Android para compartir contenido de *apps* oficiales desarrolladas por autoridades de salud pública para aplicación nacional o local (AFP, 2020). La iniciativa tiene como objetivo respetar la privacidad y seguridad del usuario mediante un sistema de datos descentralizado que utiliza *bluetooth* para notificar a los individuos si han estado en contacto con personas infectadas, al mismo tiempo proporciona sólo datos agregados a las autoridades sanitarias. Para enero de 2021, 45 aplicaciones en el mundo usan la API de Google y Apple (Woodhams, 2021). No debe dejarse de lado que estas iniciativas privadas del *big tech* han sido duramente criticadas por la imposición de estándares técnicos que dificultan la cooperación entre gobiernos y otros usuarios interesados (Clarín,

2020). Una segunda observación advierte que solo la *app* final es de código abierto, mientras que el resto de los protocolos son de acceso restringido (por razones de seguridad), lo que impide la libre “auditabilidad” del código de programación y del funcionamiento completo del sistema, lo que pone en duda los fines últimos para los cuales son *de facto* utilizados los datos por ambas compañías.

## **Cuarentena y autoaislamiento**

Las tecnologías digitales también son utilizadas para garantizar las medidas de cuarentena y aislamiento social. Entre los dispositivos y tecnologías más utilizados para este fin se encuentra el uso de códigos QR, desarrollo de *apps*, seguimiento vía GPS y circuitos de cerrados de cámaras fijas o móviles.

La ubicación de dispositivos móviles se obtiene por tres métodos principales: el uso directo del GPS, la triangulación de antenas de telecom y el WiFi (o *bluetooth*), y de manera indirecta están las numerosas *apps* digitales con acceso a los datos de ubicación GPS. En algunos casos esto se realiza con el aval de decretos oficiales aprobados a veces sin consentimiento de sus habitantes. En Ecuador, el 17 de marzo de 2020, la ministra de Gobierno, María Paula Romo, anunció que por decreto oficial el gobierno comenzaría a utilizar el rastreo por satélite para garantizar que los ciudadanos no traspasen la “valla epidemiológica”. En otros casos vemos que el seguimiento de los dispositivos para garantizar las medidas de cuarentena suele estar acompañado de otras medidas para obligar su uso y evitar el olvido de los celulares, corroborar la identidad y ubicación mediante el envío de *selfies* georreferenciadas en ciertos intervalos de tiempo. Tal es el caso de Hong Kong, que implementó una cuarentena obligatoria de 14 días para todas las personas llegadas del extranjero.

El carácter obligatorio de las medidas varía de país en país, en ocasiones su implementación se acota a sectores específicos de la población, lo cual reduce los costos de su aplicación y proporciona una mayor efectividad en el control sobre ciertos estratos de la población. En muchos casos la delimitación solo aplica a los casos confirmados del virus y en otros se incluye a las personas potencialmente positivas por haber estado en contacto cercano con los confirmados (como la mayoría de las *apps* de seguimiento de contactos); pero también suelen ser direccionadas a personas “externas” al territorio que ingresan como residentes, turistas o migrantes.

En esto se juega la determinación de los criterios “clínicos” para clasificar a las personas que en muchas ocasiones se vuelven difusos y entremezclados con juicios culturales y políticos de cada contexto situado. De esta manera existen aplicaciones marcadas por discriminaciones raciales, étnicas y de otro tipo de diferencias. Un ejemplo es Israel donde a los palestinos se les ordena descargar una *app* para verificar su salud clínica y su estado de residencia. Al mismo tiempo, los datos de sus movimientos y mensajes recibidos son enviados al ejército israelí debido (Gallagher, 2020).

Otra vía alternativa para determinar la ubicación de los móviles es la información gestionada por las corporaciones de telecomunicaciones. El gobierno de Río de Janeiro firmó un acuerdo con la empresa de telecomunicaciones TIM para utilizar datos de geolocalización de sus suscriptores para monitorear el cumplimiento de las restricciones de aislamiento. La firma transnacional Telefónica respalda proyectos gubernamentales en sus grandes mercados proporcionándoles datos geolocalizados anónimos y agregados del desplazamiento de sus usuarios: España, Brasil, Alemania y Reino Unido (Millán, 2020). Aunque existen algunos gobiernos donde las políticas de privacidad son claras y señalan explícitamente que solo les interesa analizar datos agregados, desafortunadamente en la gran mayoría de países existe un limbo donde se desconocen los detalles de la información recopilada, los fines para los que se gestiona y el tiempo por el cual el gobierno seguirá accediendo a esos datos, tal como lo advierte el grupo de trabajo Derechos digitales para la región de América Latina (Lara, 2020).<sup>8</sup>

Las cámaras vigilancia en las ciudades tampoco es tema nuevo, solo que sus funciones son reorientadas para garantizar las medidas de cuarentena y aislamiento; esto ha logrado ampliar las instalaciones, la renovación y actualización de equipos de video con tecnologías de punta en procesamiento de datos y uso de IA. Estos circuitos por lo general cerrados, tradicionalmente gestionados desde unidades centralizadas con personal de seguridad y analistas, procesan las imágenes transmitidas por las cámaras instaladas en lugares públicos. Estas herramientas a veces están directamente vinculadas con dispositivos móviles del personal policiaco para acelerar las respuestas y multar a los infractores que incumplen con el confinamiento (como en Rusia y China). Fuera de las zonas urbanas el alcance de estos sistemas es muy limitado, si acaso se extienden a aeropuertos, trenes y otras instalaciones consideradas nodos de confluencia importantes. Pero vemos también la ampliación de su foco por la generalización de drones que permite llevar el sistema de vigilancia a los cielos como nunca antes se había visto, proporcionando una vista panorámica de las ciudades a bajos costos. Los drones también son utilizados en operaciones informativas con mensajes de audio transmitidos por medio de altavoces que sirven para comunicar las medidas gubernamentales en varios países (Qatar, Brasil, México, Ecuador, Colombia y Paraguay) y para el resguardo de las fronteras y carreteras nacionales (Brasil<sup>9</sup> y El Salvador<sup>10</sup>).

---

<sup>8</sup> De acuerdo con TOP10VPN de la muestra de 120 apps en 71 países, 53% no revelan el tiempo de almacenamiento de los datos, 60% no tiene medidas de anonimato declaradas públicamente, 51% contienen seguimiento de Google y Facebook (Woodhams, 2021).

<sup>9</sup> En marzo de 2020 el Gobierno brasileño decretó el cierre temporal de la frontera con Uruguay como medida preventiva ante la pandemia y la tercera Brigada de Caballería Mecanizada del Ejército Brasileño voló un dron (DJI Mavic Mini Fly More Combo) para patrullar desde los cielos los límites fronterizos (Valadares, 2020).

<sup>10</sup> En Chaltenango, El Salvador “la policía utiliza diferentes recursos como los drones con los que alcanza una amplia visibilidad de la altura para verificar la movilidad de las personas y vehículos en las

## **Gestión clínica**

La gestión clínica se refiere al diseño de modelos de predicción que orientan la toma de decisiones clínicas al automatizar el proceso de detección de casos positivos, ubicación de hospitales o mejorar la distribución de suministros y servicios médicos disponibles. Asimismo, el desarrollo de plataformas y *apps* de atención virtual, que utilizan las videoconferencias y el monitoreo digital, se han promovido para brindar atención e información médica de manera remota. En muchos casos las *apps* digitales de rastreo y seguimiento de contactos también son *apps* que recopilan información y generan (auto)diagnósticos médicos por medio de breves encuestas virtuales, como la *app* del gobierno vietnamita, que brinda seguimiento de contactos y permite a los usuarios declarar su estado de salud y reportar casos sospechosos. En la región de América Latina, 16 países cuentan con *apps* digitales que ofrecen servicio de información médica, encuestas de síntomas para autodiagnóstico y en algunos casos se mezcla con servicios de rastreo y/o seguimiento de contactos (Ceceña y García, 2021)<sup>11</sup>. En Cuba, el gobierno promovió el uso de una *app* desarrollada por estudiantes de la Universidad de Ciencias de la Computación que colaboraron con el Ministerio de Educación Superior de Cuba, el Ministerio de Salud Pública y la empresa estatal de telecomunicaciones ETECSA con el objetivo de identificar en tiempo real aquellas personas que se auto-diagnosticaron con alguna sintomatología respiratoria y que pudieran ser sospechosas de la enfermedad. Lo anterior se realiza gracias al llenado y envío de formularios por Internet, que posteriormente son procesados y trasladados a los centros de salud (Shahbaz y Funk, 2020). Otros casos en América Latina con uso de *bots* automatizados son Panamá<sup>12</sup> y República Dominicana<sup>13</sup>.

---

calles y carreteras del país, y brindar una mejor respuesta a la emergencia nacional ante el coronavirus” (Policía Nacional Civil, 2020).

<sup>11</sup> De acuerdo con Ceceña y García (2021) las *apps* por países con función de auto-diagnóstico e información en América Latina son: Argentina (CuidAr COVID-19), Bolivia (Bolivia Segura), Brasil (Coronavirus – TOP SUS), Chile (CoronApp), Colombia (Corona App), Costa Rica (EDUS), Cuba (Pesquisador Virtual), Ecuador (ASI y SaludEC), El Salvador (e-BlueInfo), Guatemala (Alerta Guate), Haití (Haiti Strategic Health Information Systems), México (COVID Radar), Paraguay (COVID-19 PY), Perú (Perú en tus manos), República Dominicana (COVID-RD) y Uruguay (Coronavirus UY).

<sup>12</sup> El Ministerio de Salud (Minsa) de Panamá implementó la plataforma virtual de atención R.O.S.A. (Respuesta Operativa de Salud Automática) con el objetivo de poder ofrecer atención inmediata y necesaria a un mayor número de personas. El chatbot R.O.S.A. gestiona consultas digitales vía WhatsApp o a través de la línea 169 ayudando a filtrar los pacientes que presentan síntomas relacionados con la COVID-19 para ser remitidos a una atención médica. Además, responde dudas sobre la enfermedad y el virus SARS-CoV-2 (Fundación Carlos Slim, 2020b).

<sup>13</sup> “Aurora” es un bot desarrollado por el Ministerio de Salud Pública (MSP) de República Dominicana que provee información a la población sobre la COVID y conecta con más de 200 médicos, a través de herramientas sociales como WhatsApp y Telegram, permitiendo a los ciudadanos realizar video llamadas y obtener asistencia general vía telefónica o texto. En tan solo menos de 24 horas de lanzada, se reportaron más de 26 000 interacciones y 17 días después, 183 860 (Cruz y Cohn-Lois, 2020).

Los códigos QR también son usados para generar diagnósticos rápidos y semi automatizados. En China, los códigos QR recopilan información mediante breves encuestas que deben ser llenadas por los ciudadanos con datos personales (nombre, número de identidad nacional o número de pasaporte y número de teléfono). En el mismo país también se creó COVID-NET, un diseño de red neuronal convolucional profunda de código abierto disponible para médicos de todo el mundo (Whitelaw *et al.*, 2020). Esta red distingue rápidamente casos de SARS-CoV-2 de otras enfermedades pulmonares cuando se revisan las radiografías de tórax. Aunado a lo anterior, los algoritmos de aprendizaje automático desarrollados en el país asiático tienen la capacidad de predecir la probabilidad de desarrollar síndromes de dificultad respiratoria aguda entre pacientes infectados por el virus. En Brasil, la compañía de Hoobox One en conjunto con Radsquare, crearon Fevver un dispositivo que usa tecnología de IA para detectar fiebre y medir la temperatura en segundos y ha sido colocado a la entrada del Hospital Israelita de Sao Paulo (Fundación Carlos Slim, 2020a).

#### Cuadro 1.

*Principales iniciativas tecnológicas digitales para vigilar y controlar en el mundo frente a la amenaza de la COVID-19 en 2020*

	Funciones	Tecnologías digitales	Naciones que la usan
<b>Rastreo</b>	Rastrea la actividad de la enfermedad en tiempo real.	Inteligencia artificial y uso de datos en tiempo real de teléfonos inteligentes y códigos QR.	Alemania, Arabia Saudita, Argentina, Armenia, Bangladesh, Baréin, Brasil, Chile, China, Costa Rica, Cuba, Ecuador, Egipto, Emiratos Árabes, Estados Unidos, Etiopía, Georgia, Ghana, Hungría, India, Indonesia, Irán, Islandia, Jordania, Kenia, Líbano, Pakistán, Panamá, Reino Unido, Singapur, Sri Lanka, Suecia, Tailandia, Taiwán.
<b>Detección de infecciones</b>	Examina individuos y poblaciones para detectar enfermedades.	Cámaras con sensores de calor; drones; reconocimiento facial; herramientas basadas en la web y técnicas de inteligencia artificial.	Argentina, Brasil, Chile, China, Colombia, Ecuador, El Salvador, Estados Unidos, India, Islandia, Japón, México, Panamá, Perú, Singapur, Taiwán, Vietnam.

<p><b>Seguimiento de contactos</b></p>	<p>Identifica y rastrea a las personas que podrían haber estado en contacto con una persona infectada.</p>	<p>Sistemas de posicionamiento global (GPS), <i>apps</i> digitales que utilizan distintas vías para el rastreo de contactos: <i>Bluetooth</i>, GPS, Wi-Fi o códigos QR.</p>	<p>Alemania, Arabia Saudita, Australia, Azerbaiyán, Bélgica, Brasil, Bulgaria, Bután, Canadá, China, Chipre, Corea del Sur, Dinamarca, Ecuador, Emiratos Árabes, Estados Unidos, Estonia, Filipinas, Finlandia, Fiyi, Francia, Haití, Hungría, India, Indonesia, Irlanda, Islandia, Israel, Italia, Japón, Kirguistán, Kuwait, Malasia, Marruecos, México, Nigeria, Noruega, Nueva Zelanda, Pakistán, Perú, Polonia, Qatar, Reino Unido, República Checa, República Dominicana, Ruanda, Singapur, Sudáfrica, Suiza, Tailandia, Túnez, Turquía, Ucrania, Uganda, Uzbekistán, Vietnam.</p>
<p><b>Cuarentena y autoaislamiento</b></p>	<p>Identifica y rastrea a las personas infectadas y asegura medidas de cuarentena.</p>	<p>Cámaras digitales y de circuitos cerrados de tv, sistemas de GPS, uso de drones, <i>apps</i> digitales, códigos QR y localización vía empresas telecomunicación</p>	<p>Alemania, Armenia, Australia, Bahrein, Birmania, Brasil, Chile, China, Colombia, Corea del Sur, Ecuador, El Salvador, Emiratos Árabes, España, Estados Unidos, Estonia, Francia, Holanda, Hungría, India, Islandia, Japón, Kazajistán, Kenia, Malasia, Marruecos, México, Nigeria, Paraguay, Perú, Polonia, Reino Unido, Rusia, Sri Lanka, Sudáfrica, Tailandia, Taiwán, Túnez, Turquía, Ucrania, Vietnam.</p>
<p><b>Gestión clínica</b></p>	<p>Diagnostica individuos infectados, monitorea el estado clínico, predice los resultados clínicos, proporciona capacidad para servicios de telemedicina y atención virtual.</p>	<p>Inteligencia artificial para diagnóstico, plataformas de atención virtual (auto-diagnóstico) o telemedicina.</p>	<p>Alemania, Andorra, Arabia Saudita, Argentina, Australia, Bolivia, Brasil, Bulgaria, Canadá, Chile, China, Colombia, Costa Rica, Croacia, Cuba, Dinamarca, Ecuador, El Salvador, España, Estados Unidos, Estonia, Guatemala, Haití, Honduras, Irán, Irlanda, Kazajistán, Kuwait, Malasia, México, Pakistán, Panamá, Paraguay, Perú, Reino Unido, Republica Dominicana, Rusia, Tailandia, Ucrania, Uruguay, Vietnam.</p>

**Fuente:** Elaborado con información de Whitelaw *et al.* (2020), Freedom on the Net (Shahbaz y Funk 2020), COVID Tracing Tracker (MIT Technology Review 2020), Naciones Unidas (2020), Pandemic Big Brother (2020), TOP10VPN.com (Woodhams 2020), Privacy International (2020) y otras fuentes hemerográficas.

## Problematizando la cibervigilancia en el contexto de la pandemia de COVID-19

El presente texto evidencia el uso *global* de diversos mecanismos empleados con fines de vigilancia y control social durante la pandemia de COVID-19. Del cual podemos observar pautas comunes entre los países como el hecho de extender masivamente el uso ampliado de dispositivos biopolíticos de tecnología digital. Aunque su instrumentalización varía con rasgos e intereses situados, ésta dista de ser una implementación homogénea que responda a un mando centralizado. Sin embargo, el fenómeno no cumple condiciones suficientes para ser propiamente un nuevo paradigma de seguridad. Se trata más bien de la agudización, reafirmación y afianzamiento de tendencias y comportamientos previamente existentes y normalizados. De esta manera, la emergencia sanitaria complejiza las lógicas de control y vigilancia en nuestras sociedades, reformulando los mecanismos de poder y los elementos de control digital.

De ahí que coincidamos con autores que señalan que la pandemia emerge en una territorialidad previamente vigilada. La politóloga argentina Pilar Calveiro (2020) sostiene que los tiempos de biopoder anteceden la aparición del coronavirus y Juan Manuel Romero junto con William Álvarez (2021) nos recuerdan que tanto el poder que oprime como los oprimidos ya coincidían “en el deseo de vigilar y de ser vigilados” (Romero y Alvarez, 2021).<sup>14</sup> De igual forma Danielle Couch, Priscilla Robinson y Paul Komesaroff (2020) argumentan que no hay nada nuevo en el sistema de vigilancia ahora en vigor, incluso la propia visibilidad y dependencia de la participación activa de los individuos sujetos al sistema de vigilancia representa lo que Foucault denominó como “propia sujeción”, que se da a través de prácticas de autovigilancia y autodisciplina internalizadas. Mientras que las condiciones tecnológicas e incluso socio-institucionales operaban bajo lo que Shoshana Zuboff (2019) define como “capitalismo de vigilancia”: una nueva configuración del orden capitalista donde la experiencia humana con interacción de dispositivos y plataformas digitales, se convierte en materia prima sujeta a un monitoreo y observación permanente para retroalimentar prácticas comerciales basadas en la extracción, acumulación, procesamiento, estimación y modelación de la codificación binaria del comportamiento humano (Zuboff, 2019). Además, la aplicación de tecnologías digitales

---

<sup>14</sup> Los autores destacan la importancia de las redes sociales digitales. Estos autores utilizan el concepto de Gilles Deleuze y Félix Guatarri “máquina de guerra” e interpretan al virus del Sars-2 como dispositivo para estirar el campo social, en el que lo epidemiológico precede a la demografía. Adicionalmente está la implementación de la dictadura del ocio como estrategia también de aplanamiento social en el que “básicamente nos movilizan, desmovilizándonos”. Para los autores aplanar, hacer lisa la superficie, no refiere a una ausencia de elementos, sino a la facultad para agilizar “las conexiones facilitadas por las texturas y contaminaciones cromáticas”. En este caso el Estado tiene como tarea estirar el espacio sobre el que gobierna, para establecer un orden y control sobre lo que fluye en él.

para vigilar ya estaba gestionada por intereses estatales, como se observa en China. Este fenómeno también ha sido denunciado en sociedades occidentales, debido a que es considerado como una serie de prácticas de espionaje poco transparentes realizadas por agencias estatales estadounidenses como la Agencia Central de Inteligencia (CIA, por sus siglas en inglés) o la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés) en nombre de la seguridad nacional o la lucha antiterrorista, institucionalizada en la *Patriot Act*, publicada el 26 de octubre de 2001.<sup>15</sup>

Asimismo, autores marxistas apuntan a que ya existían las condiciones para que la pandemia global sucediera y señalan que era solo cuestión de tiempo. Para ellos, la emergencia de la pandemia es considerada como una mutación viral, producto de la constante y acelerada interacción de elementos biológicos-químicos en las transformaciones de flujos de materia y energía por un capitalismo globalizado hiperconectado (Wallace *et al.*, 2020; Foster y Suwandi, 2020).

Todos los elementos anteriores efectivamente yacían, no como destino sino como potencia, que únicamente logran su articulación concreta en la pandemia. Entonces, de nuevo, ¿existe algo singular en las tecnologías y dispositivos utilizados para vigilar y controlar durante la actual pandemia? De acuerdo con el balance de Juan Pablo Esperón y Ricardo Etchegaray (2021), un punto común en las reflexiones de varios filósofos destaca la instauración de “un nuevo orden mundial, un nuevo ordenamiento del espacio-tiempo, pero muchos dudan de atribuirlo a la pandemia, ya que consideran que las causas son anteriores y exteriores a ella” (2021:80). Una nueva territorialidad *global* donde la pandemia es más bien la punta de lanza que en su devenir abre camino para fortalecer la implementación masiva de tecnologías digitales como dispositivos ideales de seguridad, “un sistema de control social sin precedentes en alcance y poder” (Couch, Robinson y Komesaroff, 2020:4). A este respecto, Paul B. Preciado menciona “lo que está siendo ensayado a escala planetaria a través de la gestión del virus (SARS-CoV-2) es un nuevo modo de entender la soberanía” (Preciado, 2020), pero que al mismo tiempo, sirve para refrendar la toma de poder por la codificación de intereses estatales particulares y corporaciones transnacionales privadas mediante procesos de subjetivación, asimilación e interiorización de actitudes, perfeccionamiento de métodos y ensayos tecnológicos en mayor escala. Los dispositivos tecnológicos para vigilar y controlar en la pandemia son entonces una manifestación pública en escala global del orden reinante, de sus intereses, privilegios, desigualdades y jerarquías entre países, corporaciones transnacionales, clases sociales, géneros, razas y etnias.

---

<sup>15</sup> En 2013, Edward Snowden hizo una filtración de documentos pertenecientes a la NSA demostrando el espionaje estadounidense sobre la población estadounidense y del mundo: la NSA tenía acceso directo a la información proveniente de los teléfonos celulares en Estados Unidos. Cabe resaltar que Microsoft, Apple, Google, Yahoo, Facebook, YouTube, PalTalk, Skype, AOL contribuyen al espionaje colaborando con la NSA (Foster, 2014).

La preocupación de varios autores está en la posibilidad o no de que una vez concluida la pandemia cesen consigo el sistema de control y vigilancia actual (Barriga *et al.*, 2020). Esperón y Etchegaray (2021) advierten que es muy probable que el acontecimiento de la pandemia (la novedad, singularidad y contingencia) sea algo muy difícil de aseguir, no obstante podemos vislumbrar la consolidación del sistema de seguridad dado el gran potencial de las nuevas tecnologías y los dispositivos para administrar datos y regular el flujo de cosas, mercancías, personas; e incluso sorprenderse por la rapidez en cómo éstas se materializan, se “normalizan”<sup>16</sup> y se hacen cuerpo en los individuos (Preciado, 2020).<sup>17</sup> Para Leclercq-Vandelannoitte y Aroles (2020), la pandemia presenta una “oportunidad única” para observar el proceso de normalización de las sociedades de control que se desdobra en la lucha en contra de la COVID-19.<sup>18</sup>

## Reflexiones finales: la llamada “nueva normalidad”

La difusión del virus SARS-COV-2 y su pandemia tuvieron impactos innegables en las vidas humanas del mundo entero. Los diferentes ámbitos de las afectaciones se distribuyen de manera desigual entre las poblaciones de los países del Norte y Sur global. En la búsqueda de soluciones funcionales para el resguardo del orden, el uso de la tecnología digital se ha perfilado como la más eficiente para enfrentar y mitigar la pandemia. La investigación presentada muestra una radiografía panorámica de los diferentes usos y aplicaciones de tecnologías digitales que en su conjunto evidencian prácticas para clasificar, vigilar, disciplinar y controlar a las poblaciones. El alcance global de estos dispositivos logrado en tan poco tiempo resulta algo inédito.

Más allá de abordar el fenómeno como un asunto de violación de derechos (de privacidad, transparencia, identidad, etc.), el texto sugiere problematizar las relaciones de poder que se articulan en torno a las soluciones tecnológicas digitales y sus aplicaciones como dispositivos de control y vigilancia. En este tenor, la investigación da cuenta de la estrecha cooperación internacional entre gobiernos y

---

<sup>16</sup> Este concepto hace referencia a la inclinación natural de la población a aceptar a la sociedad de control como una realidad normal.

<sup>17</sup> Para Paul Preciado “las distintas epidemias materializan en el ámbito del cuerpo individual las obsesiones que dominan la gestión política de la vida y de la muerte de las poblaciones de las poblaciones en un periodo determinado” (Preciado, 2020).

<sup>18</sup> Para estos autores, el control continuo y la comunicación instantánea está presente en la situación actual con el uso de los dispositivos tecnológicos de control y vigilancia. Éstos materializan formas continuas y remotas de control que asumen diferentes variaciones, pero que al mismo tiempo, manifiestan la misma modulación. Como se mencionó en el marco teórico, las sociedades de control se caracterizan por el principio de “modulación”, que es posible debido a las tecnologías. Esto señala que tanto los individuos como las sociedades se encuentran fragmentadas. Así, el control siempre se reinventa a sí mismo.

corporaciones en construir narrativas que justifiquen y promuevan la implementación de dispositivos para el resguardo del orden de las cosas de la sociedad capitalista. Definitivamente esto no es un proceso homogéneo ni tampoco existen mandos únicos en su gestión; se trata más bien de dar cuenta de las lógicas de seguridad y comportamientos comunes con intereses compartidos que se articulan bajo tensiones y disputas en la territorialización de los dispositivos y los cuerpos.

Finalmente subrayamos la necesidad de seguir trabajando colectivamente en la denuncia de sus lógicas, discursos, sujetos e instituciones que reproducen los sistemas actuales de seguridad. Un trabajo colectivo que desde distintas latitudes se suma a la labor de visualizar, problematizar y politizar los dispositivos de control y vigilancia en la actualidad.

## Bibliografía

- AFP. (2020). Apple y Google usarán tecnología digital contra el Covid-19. *La Jornada*, en: <https://bit.ly/3wNwIct>
- Almenara, M. (2020). Drones para combatir el Covid-19. *Métrica Perú*, en: <https://bit.ly/32btCRs>
- Barber, G. (2020). Schools Adopt Face Recognition in the Name of Fighting Covid. *Wired*, en: <https://bit.ly/3tf9Hgm>
- Burt, C. (2020). Tokyo Olympics considering biometric facial recognition for contact tracing, NEC likely supplier. *Biometric Update*, en: <https://bit.ly/2RqTRBj>
- Cabrol, M. (2020). ¿Es la privacidad de los datos el precio que debemos pagar para sobrevivir a una pandemia? *Banco Interamericano de Desarrollo*, en: <https://bit.ly/3g5MzgQ>
- Calveiro, P. (2020). Coronavirus en tiempos de biopolítica. *La Otra Revista*, en: <https://bit.ly/3mFoFKa>
- Castro, E. (2004). *El vocabulario de Michel Foucault*. Buenos Aires: Prometeo, Universidad Nacional de Quilmes.
- CE. (2020). Cómo pueden ayudar las aplicaciones de rastreo y alerta durante la pandemia. *Comisión Europea*, en: <https://bit.ly/2RxgtAf>
- Ceceña, A. y J. García (2021). Sistemas de vigilancia digital en América Latina frente a la emergencia sanitaria. *Observatorio Latinoamericano de Geopolítica, IIEC-UNAM*, en: <https://bit.ly/3mGqUNc>
- Clarín. (2020). En Europa Aparecen las primeras críticas contra la app de Apple y Google que rastrea contactos con COVID-19. *Clarín Tecnología*, en: <https://bit.ly/3s86MER>
- Couch, D., P. Robinson y P. Komesaroff (2020). COVID-19 Extending Surveillance and the Panopticon. *Journal of Bioethical Inquiry*, en: <https://dx.doi.org/10.1007%2Fs11673-020-10036-5>

- Cruz, J. (2020). Los canales digitales en la gestión del COVID-19: El caso de República Dominicana. *Banco Interamericano de Desarrollo*, en: <https://bit.ly/3da2fgT>
- Deleuze, G. (1999). 17. Post-scriptum sobre las sociedades de control. *Conversaciones, Valencia: Pre-textos*, 277-281.
- Barriga, A. C., A. F. Martins, M. J. Simoes y D. Faustino (2020). The COVID-19 pandemic: Yet another catalyst for governmental mass surveillance? *Social Sciences & Humanities Open*
- Esperón, J. P. y R. Etchegaray (2021). Heidegger, Deleuze, el acontecimiento y el Covid-19. Diferencia(s). *Revista de teoría social contemporánea*, (12):73-82.
- Foster, J. y I. Suwandi (2020). Covid-19 and Catastrophes Capitalism. Commodity Chains and Ecological-Epidemiological-Economic Crisis. *Monthly Review*, 72(02).
- Foster, J. (2014). Surveillance Capitalism. Monopoly-Finance Capital, the Military-Industrial Complex, and the Digital Age. *Monthly Review*, 66(03):1-31.
- Foucault, M. (2006). *Seguridad, territorio y población*. Buenos Aires: Fondo de Cultura Económica. 479 p.
- Foucault, M. (2002). *Vigilar y castigar. Nacimiento de la prisión*. Buenos Aires: Siglo XXI Editores Argentina. 314 p.
- Fundación Carlos Slim. (2020a). Desarrollan en Brasil un dispositivo de Inteligencia Artificial para la detección de fiebre. *Fundación Carlos Slim*, en: <https://bit.ly/2OKNKHa>
- Fundación Carlos Slim. (2020b). El auge de las herramientas digitales en Panamá durante el brote de COVID-19. *Fundación Carlos Slim*, en: <https://bit.ly/3g1UOKN>
- Gallagher, R. (2020). Surveillance Technology Will Only Get More Intense After Covid. *Bloomberg Businessweek*, en: <https://bloom.bg/3g3wbgL>
- Gan, N. (2020). China está luchando contra el coronavirus con un código QR digital. Así funciona. *CNN*, en: <https://cnn.it/3uPVfvT>
- Holmes, O. (2020). Coronavirus mass surveillance could be here to stay, experts say. *The Guardian*, en: <https://bit.ly/3d8u3Cu>
- Ilyushina, M. (2020). How Russia is using authoritarian tech to curb coronavirus. *CNN*, en: <https://cnn.it/3g6bMaE>
- Lara, C. (2020). La vigilancia por reconocimiento facial se extiende en la región. *Derechos Digitales*, en: <https://bit.ly/3t86yPv>
- Lazzarato, M. (2006). The Concepts of Life and the Living in the Societies of Control. En M. Fuglsand (Ed.), *Deleuze and the Social*. Edinburgh University Press.
- Leclercq-Vandelannoitte A. (2020). Does the end justify the means? Information systems and control society in the age of pandemics. *European Journal of Information Systems*, 29:6, 746-761.

- Lim, G. (2020). Frustrating the State: Surveillance, Public Health, and the Role of Civil Society. *Center for Media, Technology and Democracy*, en: <https://bit.ly/3dgZryV>
- Millán, S. (2020). Telefónica extiende sus herramientas de 'big data' contra el virus a sus grandes mercados. *El País*, en: <https://bit.ly/3ecG6OD>
- MIT. (2020). Covid Tracing Tracker. MIT, en: <https://bit.ly/3dV62Ox>
- Mozur, Paul. (2019). Una red de espionaje empodera a la policía en China. *The New York Times*, 06 de abril. <https://www.nytimes.com/es/2019/12/19/espanol/vigilancia-espionaje-chino-tecnologia.html>
- Pandemic Big Brother (2020). *The pandemic gives new opportunities to Big Brother*. <https://bit.ly/2RtUNFc>
- PI Privacy International (2020). *Tracking the Global Response to COVID-19*. Privacy International. <https://bit.ly/2POv1uV>
- Preciado, P. (2020). Aprendiendo del virus. *El país*, 27 de marzo. [https://el-pais.com/elpais/2020/03/27/opinion/1585316952\\_026489.html](https://el-pais.com/elpais/2020/03/27/opinion/1585316952_026489.html)
- Riobo, A., J. Márquez y A. Calatayud (2020). Distancia2: inteligencia artificial para una movilidad más segura en época de COVID. *Moviliblog. Ideas de transporte y movilidad para América Latina y el Caribe*. <https://bit.ly/3e3nr7Q>
- Romero, J. M. y W. Alvarez (2021). La máquina de guerra nómanda del Covid-19: paisajes estéticos del epidemiocapitalismo. *Transformacao. Revista de Filosofia. Universidade Estadual Paulista/UNESP*. <https://doi.org/10.1590/0101-3173.2021.v44n4.22.p267>
- Shahbaz, A. y A. Funk (2020). *Freedom on The Net. The Pandemic's Digital Shadow*. Washington: Freedom House. <https://bit.ly/2RvokeF>
- Solís, J. (2020). Programa EDUS: la tecnología para el rastreo y apoyo de las personas enfermas ya llegó. *Delfino*, 04 de septiembre. <https://bit.ly/2RvoqD3>
- Tiqqun. (2013). La hipótesis cibernética. *Tiqqun*, en <https://tiqqunim.blogspot.com/2013/01/cibernetica.html>
- UN, United Nations (2020). *Compendium of Digital Government Initiatives in response to the COVID-19 Pandemic*. New York: United Nations. <https://bit.ly/3uReoiB>
- Valadares, R. (2020). El Ejército de Brasil emplea drones para vigilar la frontera con Uruguay. *Infodefensa*, 18 de octubre. <https://bit.ly/3uYgID1>
- Wallace, R., A. Liebman, L. F. Chaves y R. Wallace (2020). COVID-19 and Circuits of Capital. *Monthly Review*, 72(01).
- Wee, S. (2020). China Is Collecting DNA From Tens of Millions of Men and Boys, Using U.S. Equipment. *The New York Times*, 06 de abril. <http://let.iiec.unam.mx/node/2919>

- Weidenslaufer, C., M. Meza y C. Medel. (2020). COVID-19: Uso de apps con rastreo de contactos y respeto a la privacidad. *Asesoría técnica parlamentaria, boletín no.10*, 1 de julio. <https://bit.ly/3sgVEWm>
- Whitelaw, S., M. A Mamas, E. Topol y H. GC (2020). Applications of digital technology in COVID-19 pandemic planning and response. *Lancet Digital Health*, 2 (8) e435-40. <https://bit.ly/32aGxDs>
- Woodhams, S. (2021). COVID -19 Digital Rights Tracker. *TOP10VPN*, 20 de marzo. <https://bit.ly/3sb38tZ>
- Zhigulina, O. (2020). В Подмоскowie Росгвардия запустила аэростат для контроля за соблюдением режима самоизоляции. *TJournal Russia*, 16 de mayo. <https://bit.ly/3dYxnz7>
- Zuboff, S. (2019). *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*. Nueva York: Public Affairs.