Universitat de les Illes Balears

Facultad de Filosofía y letras

Memòria del Treball de Fi de Grau

Crecimiento del capitalismo de vigilancia en la Unión Europea y sus amenazas a la democracia, el ejemplo de las aplicaciones de rastreo de contactos durante la pandemia de COVID-19

Carlos Seda Gambín

Grado en Filosofía

Any acadèmic 2019-2020

DNI de l'alumne:43158069H

Treball tutelat per Bernardo Riutort Serra
Departament de Filosofía y Trabajo Social

	Autor		Tutor	
S'autoritza la Universitat a incloure aquest treball en el Repositori Institucional per a la seva consulta en accés obert i difusió en línia, amb finalitats exclusivament acadèmiques i d'investigació	Sí ☐	No ☐	Sí ☐	No ☐

Paraules clau del treball:

capitalismo de vigilancia, democracia, Unión Europea, COVID-19, rastreo de contactos

RESUMEN

La situación de emergencia provocada por la pandemia de COVID-19 ha facilitado que los gobiernos adopten herramientas de vigilancia epidemiológica que impulsan una economía basada en la recolección y tratamiento de datos a gran escala. El trabajo expone cronológicamente como Google y Apple han aprovechado su posición dominante en el mercado de los sistemas operativos móviles para crear una tecnología de rastreo de contactos que frustra el desarrollo de una solución paneuropea independiente. El análisis de este caso pretende mostrar como las grandes empresas tecnológicas amenazan la soberanía política de la Unión Europea con su colonización digital.

Palabras clave: capitalismo de vigilancia, democracia, Unión Europea, COVID-19, rastreo de contactos

ABSTRACT

The emergency situation caused by the COVID-19 pandemic has made it easier for governments to adopt epidemiological surveillance tools that drive an economy based on large-scale data collection and processing. This paper presents in chronological order how Google and Apple have leveraged their dominant position in the mobile operating system market to create contact tracing technology that frustrates the development of a pan-European stand-alone solution. The analysis of this case aims to show how large technology companies threaten the political sovereignty of the European Union with their digital colonization.

Keywords: surveillance capitalism, democracy, European Union, COVID-19, contact tracing

INDICE

INTRODUCCIÓN

Pensadores como Naomi Klein (Viner, 2020), Edward Snowden (VICE, 2020) y Yual Noah Harari (Smicht, 2020) han coincidido en cuestionarse qué tipo de mundo nos dejará la pandemia. Para dar una respuesta a esa pregunta me propongo analizar cronológicamente todos los acontecimientos que han sido determinantes para la adopción de una aplicación de rastreo de contactos dentro de la Unión Europea, pues considero que su aceptación implica importantes cambios sociales. Abordaré el tema partiendo del siguiente estado de la cuestión:

El 19 de febrero de 2020, un mes antes de que la Organización Mundial de la Salud anunciara la pandemia global por COVID-19, la Comisión Europea (2020e) presentó una estrategia de cinco años donde se definían las políticas e inversiones que se han de ejecutar para potenciar la economía basada en el tratamiento de datos dentro del territorio europeo. La necesidad de desarrollar esta estrategia se puede justificar tomando en consideración ciertos sucesos relevantes de los últimos años.

El primero se sitúa en el año 2013, cuando Edward Snowden publicó, a través de *The Washington Post* y *The Guardian* (Macaskill y Dance, 2013), algunos programas de vigilancia masiva de la Agencia de Seguridad Nacional (NSA). En los documentos de Snowden se pudo comprobar que el teléfono móvil de Angela Merkel había sido rastreado por ellos desde el año 2002, mientras que la publicación del programa «Espionnage Élysée» desveló que varios presidentes de Francia también fueron objetivos de la NSA.

Por este motivo, en el año 2014, se analizaron las informaciones sobre los programas de vigilancia de Estados Unidos y su impacto en los derechos fundamentales de los ciudadanos de la UE en un documento de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo (2014). En él se señalaba la inquietud que provoca que la vigilancia masiva se utilice «por motivos distintos a la seguridad nacional y a la lucha contra el terrorismo en su sentido estricto, como por ejemplo, para el espionaje económico e industrial o la elaboración de perfiles por razones políticas» (p. 8); además, alertaba de que los servicios en la nube ofrecidos por las principales empresas tecnológicas de Estados Unidos habían facilitado el acceso a los datos personales almacenados por los ciudadanos de la Unión Europea, y planteaba que, para

alcanzar una alta seguridad informática, era necesario desarrollar servicios en la nube europeos. Por ello, el documento concluía que: «Los europeos deben estar dispuestos a dedicar suficientes recursos, tanto humanos como financieros, a conservar la independencia y autonomía de Europa en el ámbito de la tecnología informática» (p. 25).

El segundo suceso relevante lleva desarrollándose desde los años ochenta, pues cada década ha traído consigo un salto de generación en las redes de telefonía móvil que ha implicado cambios profundos a nivel económico y social. Las redes 3G facilitaron el acceso a internet desde dispositivos móviles, después las redes 4G aportaron suficiente velocidad para permitir una interacción intensa con contenidos multimedia y servicios en la nube; pero los avances logrados por estas generaciones son ampliamente superados por las posibilidades que ofrecen las redes 5G. La Agencia Española de Protección de Datos (2020), en su informe sobre los riesgos para la privacidad de las redes 5G, señala tres funcionalidades que hacen de esta tecnología una innovación disruptiva:

La primera es que cada dispositivo conectado a la red podrá tener una configuración única en la que podrá adaptar a sus necesidades particulares parámetros como el ancho de banda o la cobertura geográfica; por tanto, un teléfono móvil tendrá una configuración de propósito general, que se diferenciará de la configuración de un coche autónomo, cuyo propósito será circular.

La segunda característica singular de las redes 5G es que con ellas se podrá conocer la posición de cualquier dispositivo conectado a la red en un espacio de tres dimensiones y con un margen de error inferior a un metro; esto es gracias al gran despliegue de puntos de acceso 5G, que harán más precisas las técnicas de triangulación mediante antenas.

Finalmente, la tercera característica deriva de la segunda; al poder posicionar con tanta exactitud cada dispositivo, las tareas de computación de la red serán realizadas lo más cerca posible de este, con lo que se consigue reducir considerablemente la latencia, alcanzando una velocidad en las comunicaciones próxima al tiempo real.

Estas tres funcionalidades, junto a un mayor ancho de banda que permite soportar hasta un millón de dispositivos conectados en un kilómetro cuadrado, ofrecen las condiciones necesarias para que se pueda desarrollar una economía basada en el

Internet de las Cosas (IdC) y en el uso de la inteligencia artificial; entendiéndose por IdC el momento donde cualquier aparato electrónico puede tener acceso a la red para recibir y enviar datos sin necesidad de que intervenga ningún ser humano. Esta disponibilidad de información es esencial para entrenar inteligencias artificiales que sirvan para automatizar la toma de decisiones, ya sea en el proceso de producción de una fábrica o la gestión de la red de semáforos de una ciudad.

Por último, el tercer suceso relevante se dio durante el año 2019, cuando comenzaron los primeros despliegues de la red 5G, donde la multinacional china Huawei pudo desplegar rápidamente su tecnología y adelantarse a las tradicionales empresas competidoras como Ericsson, Nokia, Qualcomm o Intel. La razón por la que Huawei ha conseguido posicionarse como el mayor proveedor de equipos para redes 5G es que ha sido la compañía que ha hecho más contribuciones técnicas a este estándar (Iplytics, 2019), lo cual le otorga una ventaja a la hora de implementarlas en sus productos. Que las principales compañías de telecomunicaciones hayan llegado a acuerdos con Huawei ha provocado una nueva dependencia tecnológica, no respecto a los servicios en la nube, sino a los equipos físicos que posibilitan el acceso a ellos.

La Agencia Española de Protección de Datos (2020) señala que hay un alto riesgo de impacto en la privacidad ya que se posibilitará una identificación precisa y una trazabilidad detallada de las actividades de cualquier ciudadano que use la red. Además, existe el riesgo de que el gobierno chino pueda acceder a un flujo de datos inmenso a través de una puerta trasera en los equipos de Huawei. Por ello, en mayo del 2019, Donald Trump prohibió cualquier relación comercial con la multinacional china e impidió el despliegue de sus antenas en el territorio de Estados Unidos. A raíz de las tensiones políticas ocasionadas por esta medida, durante el 2020, países como el Reino Unido y algunos Estados miembros de la Unión Europea, como Francia y Alemania, también han confirmado su veto a que las compañías de telecomunicaciones de su territorio hagan libre uso de los equipos de Huawei en las partes más críticas de la red, decisión respaldada por la Comisión Europea el 29 de enero del 2020 (2020a) al sugerir a sus miembros que diversificasen la cadena de suministro, al considerar que la dependencia de la tecnología de un único distribuidor incrementa las posibilidades de que sus vulnerabilidades sean aprovechadas para atacar partes críticas de los Estados.

Por tanto, la estrategia europea de datos (Comisión Europea, 2020e) nace históricamente entre dos tensiones que se pretenden superar: la dependencia de los servicios en la nube ofrecidos por las empresas de Estados Unidos y la dependencia de la infraestructura 5G ofrecida por la industria que se encuentra bajo el control del gobierno chino. Para lograrlo, «Europa debe encontrar su propio camino, equilibrando el amplio uso del flujo de datos a la vez que se preservan unos estándares éticos y una alta privacidad y seguridad» (p. 5). De esta premisa se concluye la propuesta más ambiciosa de la estrategia presentada por la Comisión Europea: la puesta en funcionamiento, a finales del 2021, de nueve espacios que permitan recolectar datos y ofrecerlos públicamente para su explotación en sectores estratégicos y dominios de interés público. El sector de la salud tomará un papel relevante en los meses posteriores, pero en el documento estratégico ya se explicita que «el uso de datos de medios sociales agregados y anonimizados puede ser, por ejemplo, una forma eficaz de complementar los informes de los médicos generalistas en caso de una epidemia» (p. 8).

Finalizo el estado de la cuestión del tema tratado por este trabajo señalando que el objetivo que se ha marcado la Unión Europea es similar al proceso que ya fue identificado por David Harvey (2004a) como «la lógica capitalista del imperialismo», que explica cómo el capital supera la crisis de sobreacumulación en un determinado sistema territorial a través de la producción de nuevos lugares capaces de absorber los excedentes mediante la apertura de nuevos mercados, nuevas capacidades de producción y nuevas posibilidades (Harvey, 2004c). Se puede decir que los datos se han convertido en la nueva ubicación espacial del capitalismo, y su control puede otorgar una ventaja monopolista de cara a las próximas décadas porque, como también indicó Ulrich Beck (2002a), hacer uso del conocimiento sobre el conocimiento pone en marcha una espiral de productividad que crece en velocidad al penetrar y transformar el resto de los sectores productivos, tal como demuestra la rápida expansión del *Big Data* y la inteligencia artificial en la agricultura, la industria y los servicios en la última década.

El objetivo de este trabajo será mostrar cómo la urgencia de dar una respuesta coordinada a la propagación del virus ha incrementado la dependencia de la Unión Europea de los servicios ofrecidos por las grandes empresas tecnológicas de Estados Unidos, y cómo ello puede ser determinante para el tipo de mundo que nos está esperando tras la pandemia global.

ESTUDIOS EPIDEMIOLÓGICOS QUE JUSTIFICAN EL RASTREO DE CONTACTOS

El 11 de marzo del 2020, el director general de la Organización Mundial de la Salud (OMS) anunció la situación de pandemia global por COVID-19 (Organización Mundial de la Salud, 2020). Quince días después, los miembros del Consejo Europeo (2020) se comprometieron a «hacer todo lo necesario para proteger a los ciudadanos de la UE y superar la crisis, preservando al mismo tiempo los valores y el modo de vida europeos» (p. 1). Simultáneamente, diferentes equipos de investigación del Reino Unido empezaron a desarrollar modelos matemáticos para pronosticar la evolución de la pandemia y ayudar a justificar la necesidad de las medidas que los gobiernos aplicarían posteriormente (Scientific Advisory Group for Emergencies, 2020a).

El 16 de marzo del 2020, Neil Ferguson (2020c), uno de los epidemiólogos más prominentes del Reino Unido, que defiende la estadística como instrumento para predecir el comportamiento de los seres vivos, publicó, junto a su equipo del Imperial College COVID-19 Response Team, los resultados de su modelo matemático, que contemplaba dos estrategias posibles para erradicar la pandemia:

La primera es la de mitigación, y tiene como objetivo frenar los contagios sin confinar a toda la población. Persigue la inmunidad de grupo a través de exponer a los individuos a la enfermedad; esto supone soportar un mayor número de muertes y superar ampliamente la capacidad de atención del sistema sanitario.

La segunda estrategia es la de supresión; su fin es acabar con toda transmisión de la enfermedad reduciendo su ritmo de reproducción por debajo de R1 —donde el valor 1 representa que cada persona enferma contagia a otra—, implicando un mayor coste económico y social al requerir de intensas medidas de control.

Los autores del artículo no ven asumible un escenario donde se dé la saturación de las unidades de cuidados intensivos, por eso estiman necesario implementar la estrategia de supresión, mediante una combinación de confinamiento, distanciamiento social de toda la población y cierres de escuelas y universidades.

Además, el artículo ofrece la proyección de un escenario donde las medidas de la estrategia de supresión son mantenidas hasta que se disponga de una vacuna,

permitiendo solo la apertura de escuelas y universidades junto a la relajación del distanciamiento social, siempre que las unidades de cuidados intensivos no se encuentren saturadas y no haya un ascenso rápido de contagios en el plazo de una semana. Esta proyección asume que, si se cumplen las restricciones, en los próximos dos años habrá varios brotes que afectarán a un número inferior de casos, en comparación con los que se registraron en los primeros meses de la enfermedad; esto se ajusta con los acontecimientos ocurridos hasta agosto del 2020, donde Hong Kong se está enfrentado a su «tercera ola» de contagios (De la Cal, 2020) y varios países europeos se encuentran a las puertas de la segunda.

Es necesario mencionar que este artículo consiguió un gran alcance el mismo día que fue publicado, ya que la proyección del modelo matemático que preveía 250 000 casos críticos en ausencia de medidas copó las noticias del *Financial Times* (Cookson, 2020), *The Guardian* (Boseley, 2020) o la *BBC* (Gallagher, 2020), y tuvo un efecto persuasivo inmediato en la administración de Boris Johnson, que pasó de defender la opción de la inmunidad de grupo a, una semana después, ordenar el confinamiento de toda la población.

Curiosamente, Neil Ferguson (2020a) tardó un mes en publicar el código del modelo en el que estaban basados los resultados del artículo, siendo la primera versión compartida el 22 de abril del 2020 en GitHub. Además, tuvo que admitir que había reutilizado un código de hace trece años que modelizaba una pandemia de gripe (Ferguson, 2020b). A pesar de ello, su desarrollo logró el certificado *codecheck* al superar la revisión de pares realizada por Stephen Eglen (2020), quien consiguió reproducir, con el código publicado del modelo, los mismos resultados partiendo de los mismos parámetros usados en el artículo.

El Centre for the Mathematical Modelling of Infectious Disease, un equipo de investigación de la London School of Hygiene & Tropical Medicine, también asume en su modelo matemático un escenario donde se producirán varios rebrotes a lo largo del tiempo hasta que la vacuna esté disponible (Hellewell et al., 2020), pero ofrece más detalles sobre cómo es posible controlar cada nueva propagación en un plazo de tres meses mediante el aislamiento de casos confirmados y el rastreo de contactos. El concepto «rastreo de contactos» es definido por la OMS (2017) como un proceso de vigilancia que, una vez confirmado que un individuo está infectado por un virus, intenta

identificar todas las personas con las que ha podido tener contacto directo para aislarlas y darles tratamiento temprano si desarrollan síntomas. Por contacto directo se establece cualquiera que implique una distancia menor de dos metros por al menos quince minutos (Keeling, Hollingsworth y Read, 2020). Al mismo tiempo, para que el rastreo de contactos sea efectivo requiere descubrir los casos antes de que estos se vuelvan infecciosos, por lo que su identificación debe realizarse en un tiempo más corto que el periodo de incubación (Hellewell et al., 2020). Partiendo de estas premisas, el modelo del Centre for the Mathematical Modelling of Infectious Disease realizó mil simulaciones llegando a la siguiente conclusión: en escenarios donde el ritmo de reproducción es superior a R2 —cada persona enferma contagia a dos— el 15% de los contagios ocurre antes de que se muestren síntomas y al menos el 80% de los contactos deben ser rastreados para frenar con éxito la propagación (Hellewell et al., 2020).

Los trabajos de estos dos centros de investigación fueron utilizados como referencias por los estudios del Centro Europeo para la Prevención y Control de Enfermedades (2020), institución encargada de asesorar a los gobiernos de la Unión Europea durante la crisis. Su influencia se puede comprobar en la comunicación conjunta presentada a mediados de abril del 2020 por la presidenta de la Comisión Europea (2020b) y el presidente del Consejo Europeo, donde se establecieron las medidas necesarias para permitir el levantamiento del confinamiento total, las cuales se pueden enmarcar dentro de la estrategia de supresión antes mencionada: «realización de pruebas a gran escala para detectar y vigilar la propagación del virus, combinadas con el rastreo de los contactos, y la posibilidad de aislar a la población en caso de reaparición y ulterior propagación de la infección» (p. 6).

Esta es la primera vez que una comunicación oficial de la Comisión Europea hace uso del término «rastreo de contactos» como medida para controlar la propagación de la COVID-19, con el fin de recolectar información para evaluar la eficacia de las acciones tomadas. Esto es coherente con la estrategia para potenciar el tratamiento de datos dentro del territorio europeo, pues ahora, en un contexto de crisis sanitaria, su procesamiento se vuelve útil “para modelizar y realizar predicciones de la pandemia” (p. 8).

Por tanto, se puede observar que dos modelos matemáticos han tenido un profundo impacto a la hora de establecer qué medidas políticas son necesarias para controlar la pandemia, y ambos tienen un rasgo común:

Tal como señala el Scientific Advisory Group for Emergencies (2020b), los modelos matemáticos requieren datos; si bien estos pueden provenir de anteriores pandemias o de simulaciones, solo cuando sean extraídos de un escenario real se podrá cuantificar la eficacia de las medidas adoptadas. Por ello, se puede decir que los modelos matemáticos planteados justifican una gestión neoliberal del Estado, ya que realizan explícitamente un análisis de costes y beneficios en términos económicos, donde la vida humana —o mejor dicho, el número asumible de muertes— es tratada como un valor que puede intercambiarse por beneficios sociales, como la apertura de centros económicos o la relajación del distanciamiento social. Tal como plantea Ulrich Beck (2002b), «podríamos decir que el cálculo del riesgo ejemplifica un tipo de ética sin moralidad, la ética matemática de la era tecnológica» (p. 80). En la página 23 de este trabajo, veremos que esta ética matemática es una bandera que está siendo enarbolada en los últimos años por una serie de tecnólogos y científicos de datos que creen que el acceso libre a toda información por parte de los modelos matemáticos es un bien que hay que perseguir a toda costa.

PRESCRIPCIONES PARA EL DESARROLLO DE UNA APLICACIÓN DE RASTREO DE CONTACTOS

A mediados de abril del 2020, la presidenta de la Comisión Europea (2020b) y el presidente del Consejo Europeo anunciaron que una de las medidas para controlar la pandemia iba a ser la puesta en marcha de un sistema europeo de rastreo de contactos. Considerando que para que esta medida fuera efectiva se requería de la recolección de una gran cantidad de datos, fue necesario que previamente el Comité Europeo de Protección de Datos y el Supervisor Europeo de Protección de Datos hicieran su interpretación sobre la excepcionalidad de la situación y que aclararan cómo el Reglamento General de Protección de Datos (GDPR) debía ser aplicado durante el periodo de tiempo que durara la emergencia.

Por una parte, el Comité Europeo de Protección de Datos (2020) publicó una declaración el 19 de marzo del 2020 con una serie de aclaraciones:

En el punto 1 se menciona que el artículo 6 del GDPR considera lícito el tratamiento de datos privados si es necesario para el cumplimiento de una misión realizada en interés público; también se alude al artículo 9 del mismo reglamento, que detalla que no se prohibirá el tratamiento de datos personales si es necesario por razones de interés público en el ámbito de la salud pública.

En el punto 2 se añade que los tratamientos que se hagan de los datos tendrán un propósito explícito —como el rastreo de contactos—, informando de manera transparente a los interesados sobre el uso que se esté dando de ellos e impidiendo su divulgación a terceros.

Por otra parte, el Supervisor Europeo de Protección de Datos, Wojciech Wiewiórowski (2020b), hizo pública una carta, del 20 de marzo del 2020, donde respondía a la consulta realizada por Roberto Viola, director general del Departamento de Redes de Comunicación, Contenido y Tecnología de la Comisión Europea. En ella realiza una serie de aclaraciones en torno al seguimiento de la propagación de COVID-19: Por una parte, que el uso de datos anónimos para mapear la propagación está permitido siempre que no se pueda identificar a una persona mediante ellos. Por otra, indicó que es preferible que el acceso a los datos esté limitado a los expertos en

epidemiología autorizados. Finalmente, señaló que los datos deberán ser eliminados en cuanto la situación de emergencia finalice. Estas líneas de actuación adquieren un marco el 6 de abril del 2020 con la declaración que efectuó Wiewiórowski (2020a), donde reiteró que el derecho a la protección de los datos personales debe ser equilibrado con otros derechos fundamentales; por ello se justifica que, en la situación de emergencia que plantea la pandemia, se pueda procesar datos sensibles por interés público.

Ya que la situación de excepcionalidad permitía el tratamiento de datos personales con el fin de superar la crisis de COVID-19, la Comisión Europea (2020c), el 8 de abril del 2020, anuncia una serie recomendaciones para que sus Estados miembro puedan hacer uso de aplicaciones móviles que interrumpan las cadenas de transmisión. Entre estas recomendaciones, llama la atención que se vuelve a mencionar la «estrategia europea de datos» y la necesidad de «crear un mercado único en el que los datos puedan circular en la UE y en todos los sectores, en beneficio de todos» (p. 3, punto 11), acorde con lo analizado en la primera parte de este trabajo; por ello, la Comisión Europea propone un enfoque paneuropeo en el uso de las aplicaciones por parte de los Estados miembro, garantizando su interoperabilidad.

Para lograrlo, el 17 de abril del 2020, la Comisión Europea (2020d) ofreció una serie de orientaciones para limitar la intrusión de las aplicaciones móviles y garantizar el cumplimiento del Reglamento General de Protección de Datos, tomando como referencia las aclaraciones previas del Comité Europeo de Protección de Datos y del Supervisor Europeo de Protección de Datos, que se resumen en: primero, las autoridades sanitarias nacionales serán las responsables del tratamiento de datos; segundo, se garantizará que las personas puedan instalar voluntariamente la aplicación, la cual será desactivada cuando la pandemia esté controlada; tercero, los datos que genere la aplicación solo serán compartidos con la autoridad sanitaria si se confirma que la persona está infectada y esta da su consentimiento; cuarto, no será necesario recoger los datos de localización, ya que por el principio de minimización de datos, que implica recoger los datos estrictamente necesarios para un fin preciso, no se justifica esta intrusión en la intimidad; y quinto, se debe garantizar la seguridad de los datos que almacene la aplicación, utilizando técnicas de encriptación e identificadores temporales.

En los apartados posteriores se mostrará cómo todas las recomendaciones efectuadas por la Comisión Europea a sus Estados miembros chocan con una realidad

más compleja, donde la burocracia europea no puede acceder. Por el momento, es preciso observar que cuando la Comisión Europea se cuestiona los límites de la privacidad en este periodo de urgencia, en el fondo está planteando una moción de confianza que se apoya instalando la aplicación de rastreo de contactos. Ninguna institución europea podrá garantizar con rotundidad que ningún tercero hará un tratamiento malicioso de los datos si se almacenan de manera centralizada. De ello se deduce que la única garantía real que puede ofrecer una aplicación de rastreo de contactos para ser confiable es que proteja los datos a partir de su diseño y por defecto; esto implica que la única forma de impedir todo uso no deseado es reduciendo a cero las opciones de acceder a la totalidad de los datos, o dicho de otro modo, evitar todo almacenamiento centralizado. Es importante poner atención en el desplazamiento de la confianza en una autoridad central que preserva los datos, a la confianza en un diseño descentralizado que preserva los datos. Como veremos en la página 21 de este trabajo, la tensión entre ambas opciones estuvo en el centro del debate cuando se tuvo que definir concretamente cómo debía funcionar la aplicación paneuropea de rastreo de contactos.

ESTADO DEL ARTE

Antes de que la Comisión Europea propusiera, en abril del 2020, el desarrollo de una aplicación paneuropea para el rastreo de contactos, países como China, Corea del Sur, Israel y Singapur habían puesto en marcha soluciones con el mismo objetivo, pero con enfoques y resultados diferentes. Todos los sistemas de rastreo de contactos que desplegaron estos países comparten un rasgo común: combatir la propagación del virus extendiendo la vigilancia a través de los dispositivos móviles de sus ciudadanos, con tal de conocer de manera rápida y detallada con quién había tenido contacto cada nuevo caso de contagio.

El gobierno de China fue el primero en desplegar un sistema de rastreo de contactos digital. La prueba piloto se realizó el 11 de febrero 2020 en Hangzhou, la capital de la provincia de Zheijang, donde se introdujo un sistema basado en códigos de salud de obligado uso si un individuo quería circular libremente (National Health Commission of the People's Republico of China, 2020). La elección de esta ciudad es debida a que en ella ya se encontraba implementado el proyecto *City Brain*, desarrollado por el gigante del *e-commerce* Alibaba; consiste en una inteligencia artificial que gestiona y coordina todos los servicios de la ciudad a través del tratamiento de un gran volumen de datos, por lo que, basándose en la información almacenada previamente, se podía facilitar un seguimiento de los movimientos de todos los individuos, identificar los contactos que habían realizado, tener un control de los accesos a espacios públicos y aislar rápidamente a aquellos con riesgo de haber sido contagiados (Wang et al., 2020).

El funcionamiento de los códigos de salud está basado en el sistema de pagos digitales Alipay, donde cada ciudadano dispone en su teléfono móvil de un código QR que le identifica de manera única. Así pues, cada vez que un ciudadano quiera acceder a un espacio público, debe escanear su código de salud ante un lector de códigos QR a la vez que una cámara termográfica recoge su temperatura; esta información es almacenada en el *Big Data* de la ciudad para poder disponer de un historial que es analizado en tiempo real. A partir de los datos recogidos, la inteligencia artificial asigna un color a cada código de salud —verde, amarillo o rojo— dependiendo del riesgo de exposición que se ha tenido al virus (The State Council of the People's Republico of China, 2020). La prueba piloto demostró que el gobierno podía lograr parar la cadena de

contagios entendiendo el flujo de movimiento de las personas dentro de la región y rastreando los contactos directos de cualquier individuo en un corto espacio de tiempo; por ello, el 29 de febrero del 2020, se decidió usar en toda China el sistema de códigos de salud.

El gobierno de Corea del Sur también estaba preparado, a finales de febrero de 2020, debido a la Contagious Disease Prevention and Control Act (Statutes of the Republico of Korea, 2015) el Ministerio de Salud y el Centro de Control y Prevención de Enfermedades tenían permiso para la recolección y uso de datos personales para impedir la propagación de la infección. Esta información se usaría para localizar, identificar y mandar un mensaje de alerta al teléfono móvil de toda persona que hubiera estado próxima a un contagiado, comunicándole la edad, el sexo, los desplazamientos y lugares visitados por la persona infectada (Park et al., 2020).

En junio de 2020, el gobierno de Corea del Sur siguió los pasos de China e introdujo también un sistema de códigos QR llamado KI-Pass para registrar los accesos a espacios de alto riesgo y localizar con mayor velocidad a las personas expuestas (Ministry of Health and Welfare OF South Korea, 2020).

El gobierno de Israel siguió los pasos de Corea del Sur y publicó, el 16 de marzo del 2020, una aplicación para teléfonos móviles llamada Hamagen. En su versión 1.0, la aplicación almacenaba en la memoria del teléfono los datos GPS con las fechas y tiempos donde una persona había estado los últimos catorce días (Ministry of Health of Israel, 2020b) y lo cruzaba con los datos de ubicación actualizados de los enfermos registrados por el Ministerio de Salud, lanzando una alerta al usuario cuando se ha estado expuesto (Ministry of Health of Israel, 2020a). De manera simultánea, Benjamin Netanyahu aprobó, el 18 de marzo de 2020, una medida de urgencia que permitía a la Shin Bet, la agencia de seguridad nacional de Israel, utilizar una base de datos de telecomunicaciones que hasta entonces solo se había usado para combatir el terrorismo, para comprobar si una persona sospechosa de tener el virus se encontraba realizando la cuarentena, bajo amenaza de prisión en caso de incumplimiento (Tidy, 2020).

Por su parte, el gobierno de Singapur, el 20 de marzo del 2020, lanzó una aplicación móvil llamada TraceTogether (Ministry of Health of Singapore, 2020b), que implementaba el protocolo abierto BlueTrace (Ministry of Health of Singapore, 2020a),

desarrollado por la Agencia de Tecnología del Gobierno en colaboración con el Ministerio de Salud.

Cuando un usuario se registra en TraceTogether, solo se le solicita su número de teléfono móvil y se le asigna un identificador único, anónimo y temporal; ambos datos son enviados y almacenados en un servidor central. El sistema hace uso de la conexión Bluetooth de baja energía para enviar periódicamente su identificador a los dispositivos cercanos que también hagan uso de la aplicación, los cuales almacenarán en su memoria un registro que informará si hubo una aproximación física entre sus dos propietarios durante un espacio de tiempo. Si un usuario da positivo se le pedirá permiso para enviar la información almacenada por su aplicación a un servidor central, al que tiene acceso el personal de rastreo de contactos del gobierno, quienes identificarán manualmente los encuentros de alto riesgo y enviarán una alerta a los usuarios implicados (Bay et al., 2020).

Es importante señalar que el proceso de análisis de los registros, en este caso, se realiza manualmente en un servidor central, a diferencia de la solución de Israel, que se efectúa de manera automatizada en la propia aplicación; esta diferencia de enfoque será el origen de un fuerte debate en el territorio europeo. Otro aspecto importante que se debe mencionar es que el protocolo de comunicación Bluetrace facilita la colaboración internacional al hacer interoperables las aplicaciones de rastreo que lo usen. Finalmente, hay que observar que la decisión de usar la conexión Bluetooth permite conocer con más exactitud la proximidad de las otras personas midiendo la intensidad de la señal.

Vistos los acontecimientos ocurridos hasta agosto del 2020, se puede afirmar que las diferentes soluciones planteadas han mostrado diferentes grados de efectividad. Tanto la aplicación propuesta por Israel como la de Singapur fueron incapaces de parar la propagación del virus. Además, la segunda se tuvo que enfrentar a un problema técnico que sería crucial en las decisiones que tomaría posteriormente la Unión Europea: para que pueda enviar regularmente el identificador del usuario, la aplicación debe mantenerse activa en segundo plano, aunque la pantalla esté apagada; pero Apple (2019) no permite que las aplicaciones usen la conexión Bluetooth en segundo plano en iOS, por lo que obliga a sus usuarios a mantener la pantalla encendida y la aplicación abierta, lo que hace inviable su uso por su gran consumo de batería.

Si partimos de los datos oficiales de contagios, podemos decir que el gobierno de China ha demostrado que su gestión centralizada de los datos es la solución más eficiente para frenar la propagación del virus. Ha logrado entrenar, mediante códigos QR y cámaras termográficas, a una inteligencia artificial que es capaz de monitorizar los movimientos y salud de los ciudadanos en tiempo real para lanzar alertas tempranas cuando hay posibilidad de un brote (Whitelaw, Mamas, Topol y Van Spall, 2020). Este escenario no es solo una respuesta a una crisis sanitaria, es la demostración de que China es el primer país en desarrollar ciudades completamente gestionadas por inteligencias artificiales. Un logro conseguido gracias a la tutela gubernamental que facilita la integración de todas las tecnologías que sus grandes empresas desarrollan para que todos los dispositivos puedan comunicarse entre sí; algo difícil de realizar mediante el sistema de patentes en el que se escuda la competencia en el modelo capitalista occidental. Hemos visto en la introducción de este trabajo cómo la estrategia europea de datos también tiene como horizonte construir una Unión Europea basada en el *Big Data* y la inteligencia artificial, pero a continuación se va a poder observar cómo su falta de soberanía tecnológica impide su soberanía política.

SOLUCIONES EUROPEAS

A principios de abril del 2020, dos semanas antes de que la presidenta de la Comisión Europea y el presidente del Consejo Europeo anunciaran la puesta en marcha de un sistema europeo de rastreo de contactos, dos proyectos se presentaron para liderar su desarrollo:

Por una parte, el Decentralized Privacy-Preserving Proximity Tracing (DP3T), un protocolo de comunicación mediante Bluetooth de baja energía, similar al propuesto por el gobierno de Singapur, pero con una arquitectura de datos con un elevado grado de descentralización para garantizar la privacidad de los usuarios. Por otra parte, el Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT), un consorcio que pretendía reunir a gobiernos y empresas tecnológicas para alcanzar un estándar europeo de rastreo de contactos. La colaboración amistosa de ambos proyectos durante los primeros días derivó en un agrio debate donde hubo acusaciones de opacidad y conductas deshonestas, polémica que fue interrumpida abruptamente por la sorpresiva colaboración entre Google y Apple.

El proyecto DP3T (Troncoso et al., 2020) está formado por un equipo de veintiséis investigadores, dirigidos por la española Carmela Troncoso, ingeniera de telecomunicaciones y profesora en la Escuela Politécnica Federal de Lausana, un centro de investigación suizo de donde provienen la mayoría de los miembros del grupo. Su propuesta fue publicada el 3 de abril del 2020 en la plataforma GitHub, y para elaborarla se tuvieron en cuenta las recomendaciones realizadas por el Comité Europeo de Protección de Datos y el Supervisor Europeo de Protección de Datos, que fueron analizadas anteriormente en este trabajo; el documento de presentación del proyecto resalta cuatro aspectos de su diseño que garantizan su seguridad y privacidad:

El primer aspecto es que, a diferencia de la solución ejecutada por el gobierno de Singapur, se minimizaría la recolección de datos al no almacenar en el servidor central números de teléfono ni los contactos registrados por los usuarios infectados; simplemente se guardaría una lista actualizada con los identificadores anónimos de las personas infectadas que se enviaría periódicamente a todos los usuarios del sistema, siendo la aplicación responsable de alertar cuando se ha estado físicamente cerca de un

contagiado si uno de los identificadores recibidos coincide con alguno guardado en la memoria del teléfono móvil.

A raíz de lo anterior, el segundo aspecto es que se prevendría el abuso de información, ya que todas las partes implicadas en el sistema recibirían los datos imprescindibles para su funcionamiento, impidiendo que puedan ser usados para otros propósitos.

El tercer aspecto del diseño del sistema es que prevendría el seguimiento de los usuarios no infectados, cosa que no puede garantizar la solución puesta en práctica en Singapur, ya que el almacenamiento del número de teléfono en el servidor central permite que se pueda volver a identificar a cualquier usuario cruzando datos con la información que disponen las compañías de telecomunicaciones.

Finalmente, el cuarto aspecto que garantiza la seguridad y privacidad del sistema propuesto es que es fácil de desmantelar en cuanto finalice la crisis sanitaria; los datos almacenados en el servidor son eliminados a los catorce días y el usuario solo debe parar de usar la aplicación para dejar de enviar datos.

El consorcio PEPP-PT (2020a) hizo pública su web el 1 de abril del 2020 y en ella no se presentó ningún documento técnico ni ningún código fuente para ser auditado. En vez de ello, planteaba dar asistencia a las iniciativas nacionales para que adoptaran una tecnología estandarizada para el rastreo de contactos que respetara el Reglamento General de Protección de Datos, y que permitiera su interoperabilidad entre los Estados miembros de la Unión Europea. Entre las instituciones que lideraban la propuesta estaban las alemanas Fraunhofer Heintich Hertz Institute for telecoms (2020) y el Robert Koch-Institut, que ya habían empezado a desarrollar un protocolo de rastreo de contactos centralizado llamado NTK para el gobierno alemán. Como creador y portavoz del proyecto, se presentó Hans-Christian Boos, un emprendedor alemán y miembro del Digital Council of the German Federal Government.

El 10 de abril del 2020, en la página de inicio del PEPP-PT (2020b) se hizo mención al proyecto DP3T:

> «En PEPP-PT apoyamos enfoques centralizados y descentralizados para que cada país elija el adecuado para su legislación. El enfoque DP3T es el

> proyecto que actualmente se encuentra en revisión para una implementación descentralizada».

La colaboración parecía provechosa para ambas partes. El consorcio PEPP-PT conseguía, al promocionar el trabajo realizado previamente por los miembros de DP3T, vincular su actividad a un documento técnico y a un robusto código fuente que generaba titulares en los medios de comunicación. Pero, al mismo tiempo, se dejaba abierta la puerta a una aplicación de rastreo de contactos centralizada, delegando en cada Estado la elección entre una u otra, cuando lo que se pretendía era dar una solución única a todos los miembros de la Unión Europea. Por tanto, el choque entre ambos proyectos tenía que ocurrir; es así como el día 16 de abril del 2020, la web del consorcio PEPP-PT (2020c) retiró toda mención al proyecto DP3T y comenzó el cruce de acusaciones entre aquellos que querían apostar por una arquitectura de datos centralizada y los que defendían la opción descentralizada.

El día 17 de abril del 2020, Hans-Christian Boos dejó claras sus intenciones manifestando que estaba a favor de una solución centralizada para Alemania en una entrevista en *Der Tagesspiegel* (Dalg, 2020). Sin embargo, la propuesta que estaba apoyando —el protocolo NTK, por encargo del gobierno alemán— empezó a recibir críticas a través de las redes sociales de los miembros del proyecto DP3T, donde Kenneth Paterson (2020) tomó un papel muy activo al acusar al consorcio PEPP-PT de estar apoyando un proyecto opaco, del cual no se había publicado ningún código fuente para ser auditado por otros investigadores, ni compartido sus especificaciones técnicas para que pudieran ser discutidas por la opinión pública.

Hay que mencionar que el documento de presentación del proyecto DP3T (Troncoso et al., 2020) observa con preocupación que “un sistema centralizado revela al servidor el grafo de interacciones de un usuario infectado” (p. 18), y que con cada nuevo caso se redefinen y multiplican las aristas de todos los vectores, alcanzando rápidamente una visión bastante completa del total de interacciones de la sociedad sin necesidad de almacenar las interacciones de todos los individuos. En una situación así se puede identificar a cualquier usuario aunque use pseudónimo, y se facilita que los datos puedan ser usados para fines de vigilancia. Sorprendentemente, el propio Hans-Christian Boos no rechaza este punto en la entrevista concedida el 22 de abril del 2020

a *El Confidencial* (Mendez, 2020), reconociendo que el grafo social «es lo que los epidemiólogos están pidiendo» y llama la atención que diga que por su contenido técnico «toda esta polémica se debería realizar de forma privada» dando por buenas las acusaciones de opacidad.

La polémica entre las dos posturas finalizó después de cuatro sucesos que dieron un espaldarazo definitivo a la solución descentralizada: Ante todo, y como veremos con más detalle en el próximo apartado de este trabajo, la histórica colaboración entre Google y Apple, anunciada el 10 de abril del 2020, que ofrecía a todos los gobiernos una solución propia (Google, 2020c). A continuación, la publicación el 16 de abril del 2020 del documento desarrollado por la Comisión Europea (2020d) que debía servir de guía a los Estados miembros que desarrollaran sus propias aplicaciones de rastreo de contactos, donde se reconocía que una solución descentralizada era coherente con el principio de minimización de datos. Por otra parte, los conflictos dentro del consorcio PEPP-PT provocaron que el 17 de abril del 2020 algunos miembros del parlamento europeo por el partido Renew Europe (Veld, 2020) empezaran a exigir transparencia a Hans-Christian Boos con el fin de que explicara por qué mostraba tanto interés en defender el almacenamiento centralizado de contactos, cuando el consorcio no había publicado ningún código que pudiera ser analizado por expertos. Finalmente, ese mismo día, el Parlamento Europeo (2020) aprobó una resolución donde se coordinaron las acciones de la Unión Europea para combatir la pandemia, que en su punto 52 desaconsejaba completamente el almacenamiento de datos en un servidor central por el potencial riesgo de abuso.

Podemos decir que la postura del gobierno alemán fue coherente con la estrategia europea de datos presentada en febrero, ya que facilitó que el consorcio PEPP-PT actuara como un *lobby* para forzar la creación de un espacio de recolección de datos de salud europeo, aprovechando el protocolo de rastreo de contactos centralizado que ya estaban desarrollando sus centros de investigación. El equipo de investigadores del DP3T consiguió parar este primer intento de impulsar el *Big Data* en Europa defendiendo el valor de la privacidad como garantía de la libertad individual, recuperando una definición similar a la que proponía John Locke (2006), como un derecho natural: «que hace que cada hombre tenga una propiedad que pertenece a su propia persona; a la cual nadie tiene derecho, excepto él mismo» (p. 34).

Es importante señalar que el peso que ha tenido la interpretación liberal de la privacidad en la polémica entre DP3T y PEPP-PT es clave para entender una nueva forma de capitalismo que pone a su servicio el *Big Data* y la inteligencia artificial. Shoshana Zuboff (2019b) lo llama capitalismo de vigilancia, y se caracteriza tanto por su capacidad de extraer la plusvalía a la fuerza de trabajo de una manera más eficiente, como por su capacidad de lograr extraer nuevas plusvalías, transformando el comportamiento en una nueva materia prima mediante la «dataficación»; mecanismo por el cual los individuos son incorporados a un agregado estadístico cuyo valor dependerá de la cantidad de patrones de conducta que sea capaz de pronosticar.

El capitalismo de vigilancia también tiene sus ideólogos. Como se dijo al final del segundo apartado de este trabajo, en los últimos años han tomado relevancia una serie de tecnólogos y científicos de datos que creen que el acceso libre a la información por parte de los modelos matemáticos es un bien que hay que perseguir a toda costa. En el mismo apartado, se presentó al epidemiólogo inglés Neil Ferguson como un defensor de la estadística como instrumento para predecir el comportamiento de los seres vivos; pero, sin duda, el representante más importante de esta corriente de pensamiento es Alex Pentland (2015c), profesor del MIT y defensor de la física social, la cual define como una ciencia cuantitativa que describe cómo la información y el flujo de ideas establecen conexiones matemáticas estables con el comportamiento de las personas, formando patrones de experiencia humana que son objeto de análisis de esta disciplina. La física social parte del hecho de que casi todas nuestras acciones del día a día son habituales, basadas principalmente en lo que hemos aprendido al observar el comportamiento de los demás; por ello, Pentland (2015a) defiende que, si cuantificamos las interacciones directas, podemos obtener una medida muy precisa de la presión social ejercida entre las personas, con la cual podemos pronosticar si un comportamiento nuevo permanecerá en el tiempo. Además, Pentland (2015b) calcula que si complementamos la información anterior, con estudios de movilidad que revelen los patrones de movimiento de la ciudad y estudios que identifiquen patrones en los hábitos de compra, podremos tener un conocimiento del 90% de los comportamientos, posibilitando producir predicciones de la probabilidad de que un individuo adopte un comportamiento particular.

Como se puede ver, las ideas de Alex Pentland encajan perfectamente en un capitalismo basado en el *Big Data* y la inteligencia artificial, donde el rastreo de contactos, el almacenamiento de ubicaciones y el análisis de las comunicaciones ya están en manos de las grandes empresas tecnológicas de EE. UU. Esta concentración de capacidad computacional no solo pone en peligro la privacidad del individuo, también es el origen de una importante desigualdad social (Zuboff, 2019a). En el siguiente apartado veremos como el verdadero ganador al bloquear la posibilidad de construir un *Big Data* europeo ha sido Google-Apple que, mediante su posición tecnológica dominante, que les hace dueños de prácticamente todos los sistemas operativos móviles del planeta, han podido imponer su solución en cuestiones que atañen a la salud pública, estableciendo una peligrosa intromisión antidemocrática en las decisiones de la Unión Europea.

SOLUCIÓN DE GOOGLE Y APPLE

Cuando Google y Apple anunciaron, el 10 de abril del 2020, su colaboración para ofrecer a todos los gobiernos un sistema de rastreo de contactos interoperable entre los usuarios de sus sistemas operativos, se evidenció que en el siglo XXI las instituciones democráticas son desbordadas por las intromisiones de las grandes empresas tecnológicas. Tal como fue predicho en el Senado francés por Morin-Desailly (2013), la Unión Europea se está convirtiendo en una «colonia digital» de Estados Unidos.

La relación de Google con el ámbito de la salud pública no es nueva; es necesario mencionar dos momentos previos:

El primero ocurrió en el año 2009, cuando algunos científicos de Google presentaron el algoritmo *Google Flu Trends* (Google, 2009), el cual detectaba cuando se producía un aumento de búsquedas relacionadas con la gripe para pronosticar los lugares donde se iban a producir brotes. El equipo de Google (Ginsberg et al., 2009) aprovechó los datos extraídos mediante su motor de búsqueda para compararlos con los datos de propagación de la gripe entre 2003 y 2008 aportados por el Centro para el Control y la Prevención de Enfermedades de EE.UU y, mediante el procesamiento de 450 millones modelos matemáticos, concluyeron que 45 términos de búsqueda presentaban una correlación fuerte con los datos de propagación de la gripe. Este primer intento de aprovechar el *Big Data* para realizar vigilancia epidemiológica sin necesidad de análisis médicos resultó tan asombroso como erróneo, ya que en febrero del 2013 el algoritmo pronosticó el doble de casos de los que las autoridades sanitarias detectaron realmente.

Un primer análisis publicado en *Nature* (Butler, 2013) señalaba que el desfase entre los casos pronosticados y los reales estuvo influenciado por los medios de comunicación, que dieron una gran cobertura a la temporada de gripe, provocando un cambio en el comportamiento de búsqueda de los usuarios. En cambio, un segundo análisis publicado en *Science* (Lazer et al., 2014) indicó que el problema se encontraba en un sobreajuste del modelo, el cual empleaba 50 millones de búsquedas en Google sobre 1152 observaciones del Centro para el Control y la Prevención de Enfermedades de EE.UU, provocando que el algoritmo pudiera realizar predicciones exitosas cuando se ajustaban a las características precisas de los datos usados, pero fallando al enfrentarse a una situación nueva como la excepcional aparición de la gripe porcina en 2009 o la amplia

cobertura mediática del 2013. Este último artículo mostró en sus conclusiones el camino para los futuros desarrollos de Google: no se puede crear un modelo de vigilancia epidemiológica a partir de los datos generados por una herramienta que ha sido desarrollada con otro propósito y que continuamente se está modificando, ya que no ofrece una medición experimental estable.

Un segundo momento en la relación de Google con el ámbito de la salud pública ocurrió el 3 de abril del 2020. Aprovechando los datos agregados generados por los usuarios de la aplicación Google Maps, la compañía actualizó diariamente un estudio para 131 países que ofrecía varios gráficos de tendencias de movilidad (Google, 2020g). Los datos revelaban los cambios en la cantidad de visitas a los lugares categorizados en comparación con días de referencia que representaban el valor normal y esperado para cada día de la semana, siendo un día de referencia el valor medio del periodo de cinco semanas comprendido entre el 3 de enero y el 6 de febrero del 2020 (Google, 2020d). Este estudio pretendía servir de ayuda a las autoridades durante la pandemia, para que pudieran comprender los desplazamientos que estaba efectuando la población y diseñar de manera más eficiente los horarios del transporte público (Google, 2020f). Con estos objetivos, se evidenció la estrecha relación que hay entre la identificación de patrones de movilidad y la planificación de las infraestructuras urbanas. Como en el caso del proyecto *City Brain* de la ciudad china de Hangzhou, mencionado en la página 15 del presente trabajo. Podemos ver que Google ha demostrado que, gracias a la presencia de su sistema operativo Android en la gran mayoría de dispositivos móviles de la población, pueden disponer de los datos necesarios para entrenar a inteligencias artificiales capaces de gestionar los servicios de una ciudad (Google, 2019).

Con los dos precedentes mencionados, llegamos al 10 de abril del 2020, cuando Google (2020c) y Apple anuncian su colaboración para desarrollar juntos un sistema de rastreo de contactos. Considerando que dentro del territorio europeo el sistema operativo Android tiene una cuota de mercado del 73% y el sistema operativo iOS de un 25% (Statcounter, 2020) la alianza de ambas compañías eclipsaba las soluciones que se habían presentado hasta entonces. El portavoz del consorcio PEPP-PT, Hans-Christian Boos, que defendía de manera firme el protocolo centralizado NTK promovido por el gobierno alemán, opinó lo siguiente:

> «Es genial que Apple y Google se unan y hagan algo, pero creo que no deberían decir a los Gobiernos qué deben hacer. Ya son dueños de los sistemas operativos, y no estoy seguro de que sea una buena idea que sean dueños de otras cosas. Creo que quieren ayudar y no aumentar su poder, pero también creo que ellos mismos deberían ofrecer elección. ¿Quiénes son ellos para decidir cómo deben gestionar los Gobiernos sus sistemas sanitarios?» (Méndez, 2020).

Por su parte, la líder del equipo DP3T, Carmela Troncoso, que defendía un protocolo descentralizado con tal de preservar la privacidad de los ciudadanos europeos, opinó que:

> «Tienen un poder enorme. Han tomado una decisión que limita qué puede decidir un gobierno, y puede entenderse como un problema para la soberanía. […] La mayor preocupación es que hayan tenido tanto poder para decidir qué tipo de sistema se va a implementar en el planeta. Eso da miedo. Deberíamos reflexionar como sociedad cuándo les hemos dado ese poder» (Pérez Colomé, 2020).

Podemos observar que ambos portavoces coinciden en un mismo punto: Google y Apple demostraron que tienen un poder de decisión que está por encima de la soberanía política de los gobiernos, porque son dueños del espacio virtual —el sistema operativo— que envuelve y dinamiza las interacciones que ocurren en el espacio físico. Su decisión fue firme: impusieron una arquitectura de datos descentralizada para su protocolo de rastreo de contactos.

La propuesta de Google (2020h) y Apple se inspira en la solución planteada por DP3T (Troncoso et al., 2020), que se explicó en el apartado anterior: una solución descentralizada, donde la lista de contactos de riesgo que haga el usuario quedará únicamente almacenada y cifrada en su propio dispositivo, por lo que el grafo social no podrá ser procesado por un servidor para que las autoridades sanitarias aprovechen los datos con fines epidemiológicos.

La novedad aportada por Google y Apple respecto a la propuesta de DP3T se encuentra en dos aspectos técnicos que facilitan la interoperabilidad entre los usuarios y la implementación por parte de los gobiernos:

Por una parte, el paquete de información enviado a través del Bluetooth de baja energía se llama «*beacon*», y hasta ahora existían dos protocolos de *beacons* incompatibles entre sí: el *iBeacon* creado por Apple y *Eddystone* desarrollado por Google. La primera aportación técnica de la colaboración ha sido la estandarización de un protocolo de *beacons* que permitirá que los usuarios de iOS y Android intercambiar identificadores entre sí (Google, 2020e).

Por otra parte, la solución de Google y Apple no se basa en el desarrollo de una aplicación. En una primera fase, lo que ofrecen a los gobiernos es la activación de un servicio de detección de contactos en sus sistemas operativos que facilita que las aplicaciones que desarrollen los gobiernos puedan hacer uso del protocolo de *beacons* estandarizado previamente mencionado, por lo que usuarios de distintos países pueden utilizar el mismo sistema de rastreo de contactos aun usando aplicaciones diferentes (Google, 2020b). En una segunda fase, Google y Apple quieren que no sea necesario instalar ninguna aplicación, sino que en sus sistemas operativos ya esté integrada por defecto la funcionalidad de rastreo de contactos para garantizar que todos los usuarios la tengan siempre disponible (Whittaker y Etherington, 2020). El objetivo perseguido es que su solución tenga una amplia penetración en la población, ya que en un estudio donde IBM aportó sus modelos matemáticos (Hinch et al., 2020) se llegó a la conclusión de que sería necesario que por lo menos el 56% de usuarios lo use para poder erradicar la cadena de contagio.

Tres días después del anuncio, representantes de ambas compañías aclararon en una entrevista en *Techcrunch* (Whittaker y Etherington, 2020) que su servicio de detección de contactos solo podría ser accesible por las aplicaciones desarrolladas por los gobiernos, impidiendo el uso a las aplicaciones desarrolladas por iniciativas privadas. En este momento algunos países de la Unión Europea, principalmente Alemania y Francia, tuvieron que tomar una decisión sobre si seguir adelante con sus protocolos de rastreo de contactos centralizados o, por el contrario, adoptar el protocolo propuesto por Google y Apple. El principal problema era una cuestión técnica que ya ha sido mencionada la página 17 de este trabajo: la política de privacidad de Apple (2019) no

permite que las aplicaciones usen la conexión Bluetooth en segundo plano, por lo que las soluciones centralizadas desarrolladas por los gobiernos francés y alemán obligaban a los usuarios de iPhone a mantener la pantalla encendida y la aplicación abierta para poder funcionar. En cambio, y aquí está la clave del asunto, la solución descentralizada propuesta por Apple y Google sí que permitía utilizar la conexión Bluetooth en segundo plano, facilitando su adopción por parte de toda la población. Ante esta disyuntiva, a finales de abril del 2020, el gobierno francés (Kelion, 2020) y alemán (Busvine y Rinke, 2020) intentaron negociar con Apple para que modificase su política de privacidad. La respuesta negativa de la compañía provocó dos salidas distintas: Francia decidió continuar con el despliegue de su protocolo centralizado con tal de proteger su soberanía; en cambio Alemania abandonó el consorcio PEPP-PT y aceptó utilizar el sistema de Google y Apple. Una escisión en los dos principales socios de la Unión Europea que acababa con el proyecto de construir una solución paneuropea.

Es un punto de inflexión importante que, en una situación de emergencia sanitaria, Google y Apple puedan imponer sus políticas técnicas a los Estados miembros de la Unión Europea, impidiendo que puedan desarrollar libremente una solución soberana. Tal como fue observado por Ulrich Beck (2002c), el poder de la tecnología se basa en que su puesta en práctica es mucho más rápida que la acción política, que debe vencer múltiples resistencias para llegar a acuerdos; esto permite a la tecnología imponer sus ritmos a los políticos y a la opinión pública, además de dejar en manos del criterio de los ingenieros la evaluación y prevención de desastres: «la sociedad industrial ha producido una "democracia truncada" en la que las cuestiones del cambio tecnológico social quedan fuera del del alcance de la decisión político-parlamentaria» (Beck, 2002d). El procedimiento legislativo, el tradicional método de decisión de la Unión Europea, se ve desbordado cuando sus instituciones no tienen ningún tipo de control sobre el código fuente que hace funcionar las tecnologías adoptadas por los ciudadanos europeos.

Tal como indica el colectivo de activistas Xnet (2020), no es posible garantizar que no haya una línea de código en Android o iOS que permita extraer y transferir regularmente a los servidores de sus compañías los datos recogidos por sus dispositivos móviles. Por ejemplo, según la documentación de Android (s.d), cuando el usuario da permiso al sistema operativo de su dispositivo móvil para que el sistema de rastreo de contactos utilice la conexión de Bluetooth de baja energía —ACCESS_FINE_LOCATION— también

le da permiso para determinar en cualquier momento su ubicación —ACCESS_COARSE_LOCATION—. Por tanto, cuando Google (2020a) afirma que no recolecta datos con su sistema de rastreo de contactos, la única posibilidad que le queda al usuario es confiar en esta compañía; algo difícil si se recuerda la investigación realizada por *Associated Press* (Nakashima, 2018) que demostró que los dispositivos Android y iPhone almacenaban los datos de localización aunque no tuvieran permiso del usuario.

En la página 14 de este trabajo se señaló que era importante poner atención en cómo la confianza del usuario se ve desplazada en el paso de una arquitectura de datos centralizada a una descentralizada. La primera pide al usuario que confíe en las buenas intenciones de la autoridad a la cual debe transferir sus datos y la segunda pide que confíe en la seguridad y privacidad que le promete un diseño técnico que, por defecto, está orientado a diseminar los datos. Pero, si el código fuente de una arquitectura de datos descentralizada no es público, la confianza del usuario se vuelve a depositar en una nueva autoridad, en el creador y propietario de dicho código, que promete no ejecutar funciones a espaldas del usuario. En esta situación, parece que el principio de protección de datos desde el diseño y por defecto que exige el artículo 25 del Reglamento General de Protección de Datos (2016) se ve comprometido, pero aun así la propuesta de rastreo de contactos de Google y Apple tuvo el respaldo inicial del Supervisor Europeo de Protección de Datos, el cual afirmó que: «después de una rápida mirada, parece marcar las casillas correctas en cuanto a la elección del usuario, la protección de datos por diseño y la interoperabilidad paneuropea» (BBC News Mundo, 2020). A partir de entonces, ya no había ningún impedimento, por lo que Alemania, Croacia, Dinamarca, Estonia, Países Bajos, Polonia, Portugal, Irlanda, Italia, Austria, Letonia y España decidieron implementarla en sus sistemas de salud (Parlamento Europeo, 2020b). La Unión Europea pasó a estar en manos del capitalismo de vigilancia.

Shoshana Zuboff (2019c) indica que el capitalismo de vigilancia viene acompañado de una forma de poder que denomina «instrumentalismo»; lo define como la instrumentalización de la conducta con fines de modificación, predicción, monetización y control. No es una forma de totalitarismo, pues no opera a través de la violencia; no quiere dominar el interior de la persona, solo le interesa capturar todos los datos de su comportamiento, que todo lo que haga sea accesible para ser modificado. Yuval Noah

Harari (2019) también identifica este nuevo tipo de poder y señala que está impulsado por un nuevo tipo de ideología que nombra «dataísmo», que «sostiene que el universo consiste en flujos de datos, y que el valor de cualquier fenómeno o entidad está determinado por su contribución al procesamiento de datos» (p. 400), por lo que la aparición de las inteligencias artificiales, y su capacidad de detectar patrones matemáticos a partir de grandes volúmenes de información, representa un avance destinado a sustituir la capacidad de decisión humana.

Así pues, cuando los gobiernos europeos se lanzan a los brazos de la solución de Google y Apple, ceden a ese poder instrumental para escapar de la incertidumbre social que provoca la pandemia, esperando que la tecnología introduzca certeza con sus predicciones e incluso sea capaz de tomar decisiones. Estamos ante el mundo deseado por Alex Pentland cuando defiende que la verdad computacional debe reemplazar necesariamente a la política como fundamento para la gobernanza instrumental: «Tener una ciencia matemática y predictiva de la sociedad que incluya tanto las diferencias individuales como las relaciones entre individuos […] tiene el potencial de cambiar drásticamente la forma en que los funcionarios gubernamentales, los gerentes de la industria y los ciudadanos piensan y actúan...», ese es el poder que ahora mismo tiene Google dentro de la UE.

Si los gobiernos de la UE son incapaces de desarrollar su propia estrategia de datos que garantice su soberanía política, y ceden poco a poco al poder «instrumental» de las grandes empresas tecnológicas de EE. UU, es posible que tarde o temprano sus inteligencias artificiales arrebaten incluso el monopolio de la seguridad a los Estados. Un ejemplo de esto ocurrió en enero del 2020, momento en el que Google anunció que empezaría a cobrar entre 45 y 245 dólares por cada solicitud de información privada que recibiera por parte de un gobierno (Gabriel, Dance y Valentino-DeVries, 2020) ante el continuo aumento de solicitudes (Google, s.d).

La UE está perdiendo el tren de la innovación y cada vez se encuentra más acorralada por dos bloques que disfrazan su capacidad de control como inofensiva tecnología. El despliegue de las redes 5G durante esta década traerá consigo la introducción de los coches autónomos; Google ya está empezando a despuntar con su flota de taxis *Waymo* (s.d) en Arizona ¿La UE permitirá la conquista de sus ciudades? ¿Dejará circular por sus calles inteligencias artificiales armadas con tecnología LIDAR —uso de láser para mapear

los 360 grados del espacio con márgenes de error mínimos— y cámaras de reconocimiento? Es algo que ya están haciendo los coches de Google Street View (Simonite, 2017). ¿Y si una flota de coches autónomos de Google demuestra ser un sistema de vigilancia para la ciudad más barato y eficiente que las propias fuerzas de seguridad de los Estados? ¿Cederán de nuevo los miembros de la UE como lo hicieron con su sistema de rastreo de contactos? Estos son los retos a los que nos enfrentamos en los albores del capitalismo de vigilancia.

CONCLUSIONES

El análisis cronológico de los acontecimientos que han sido determinantes para la adopción de una aplicación de rastreo de contactos dentro de la Unión Europea permite concluir que la capacidad de recolección y tratamiento masivo de datos está haciendo emerger un poder hasta ahora nunca visto por el ser humano. Las tecnologías que lo posibilitan se encuentran bajo el control de unas pocas manos, las cuales aprovechan su acceso exclusivo a la información generada para alcanzar ventajas competitivas crecientes frente al resto de actores sociales que no pueden acceder a ella.

El uso de los datos y la inteligencia artificial para automatizar la gestión de los servicios públicos de las grandes ciudades ha comenzado a ser puesto en práctica en China, y parece ser previsible que otros países seguirán su modelo ante las evidentes ventajas que aporta tener una visión global de los movimientos de la población. La pandemia por COVID-19 ha sido aprovechada para flexibilizar los reglamentos de protección de datos y presentar las tecnologías de rastreo como un bien común, es relativamente sencillo utilizar el mismo argumento cuando se quiera extender a todo servicio público optimizable.

La Unión Europea tiene una posición muy difícil debido a su dependencia tecnológica, no tiene la capacidad industrial de China que, en un corto plazo de tiempo y bajo un mando único, ha generado su propio ecosistema tecnológico al margen de Estados Unidos. Por tanto, existe el peligro de que grandes empresas tecnológicas como Google introduzcan progresivamente sus herramientas en la gestión de los servicios públicos al carecer de competidores en el territorio europeo, pudiendo ofrecer tanto una plataforma para la educación virtual como un sistema de gestión de emergencias.

Si la Unión Europea permite que las grandes empresas tecnológicas de Estados Unidos puedan controlar los datos generados por los servicios públicos de sus Estados miembros inevitablemente se encontrará con una nueva forma de colonialismo que afectará a su soberanía política. Por ello, es importante hacer un seguimiento de este proceso, en él no sólo está en juego la privacidad del individuo también el futuro de una sociedad que decide ponerse en manos de la inteligencia artificial.

REFERENCIAS BIBLIOGRÁFICAS

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2020). *Introducción a las tecnologías 5G y sus riesgos para la privacidad*. Recuperado de https://www.aepd.es/sites/default/files/2020-06/nota-tecnica-privacidad-5g.pdf

ANDROID. (s.d). Request location permissions. Recuperado de https://developer.android.com/training/location/permissions

APPLE. (2019). Location Services Privacy Overviw: IBeacon privacy. Recuperado de https://www.apple.com/privacy/docs/Location_Services_White_Paper_Nov_2019.pdf

BAY, J., KEK, J., TAN, A., HAU, C. S., YONGQUAN, L., TAN, J., Y QUY, T. A. (2020). BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders. *Government Technology Agency-Singapore, Tech. Rep*. Recuperado de https://bluetrace.io/static/bluetrace_whitepaper-938063656596c104632def383eb33b3c.pdf

BBC NEWS MUNDO. (11 abril 2020). Coronavirus: el plan de Apple y Google para rastrear el covid-19 desde tu teléfono. *BBC*. Recuperado de https://www.bbc.com/mundo/noticias-52251843

BECK, U. (2002a). ¿Conocimiento o desconocimiento? Dos perspectivas sobre la "modernización reflexiva". Dentro de La sociedad del riesgo global (p.179). Madrid: Siglo XXI.

BECK, U. (2002b). El cálculo del riesgo: seguridad predecible frente a un futuro abierto. Dentro de La sociedad del riesgo global (p.80). Madrid: Siglo XXI.

BECK, U. (2002c). El papel de la tecnología y de las ciencias naturales en la sociedad del riesgo. Dentro de La sociedad del riesgo global (p.96). Madrid: Siglo XXI.

BECK, U. (2002d). La utopía de la democracia truncada. Dentro de La sociedad del riesgo global (p.110). Madrid: Siglo XXI.

BOSELEY, S. (16 marzo 2020). New data, new policy: why UK's coronavirus strategy changed. *The Guardian.* Recuperado de https://www.theguardian.com/world/2020/mar/16/new-data-new-policy-why-uks-coronavirus-strategy-has-changed

BUSVINE, D. Y RINKE, A. (26 abril 2020). Germany flips to Apple-Google approach on smartphone contact tracing. Reuteurs. Recuperado de https://www.reuters.com/article/us-health-coronavirus-europe-tech/germany-flips-on-smartphone-contact-tracing-backs-apple-and-google-idUSKCN22807J

BUTLER, D. (14 febrero 2013). When Google got flu wrong. *Nature,* 494, 155–156*.* doi:10.1038/494155a

CENTRO EUROPE PARA LA PREVENCIÓN Y CONTROL DE ENFERMEDADES. (2020). *Coronavirus disease 2019 (COVID-19) pandemic: increased transmisión in the EU/EEA and the UK*. Recuperado de: https://www.ecdc.europa.eu/sites/default/files/documents/RRA-seventh-update-Outbreak-of-coronavirus-disease-COVID-19.pdf

COMISIÓN EUROPEA. (2020a). *Despliegue seguro de la 5G en la UE* (COM/2020/50). Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM:2020:50:FIN

COMISIÓN EUROPEA. (2020b). *Hoja de ruta europea para el levantamiento de las medidas de contención del coronavirus.* Recuperado de https://ec.europa.eu/info/sites/info/files/joint_eu_roadmap_lifting_covid19_containment_measures_es.pdf

COMISIÓN EUROPEA. (2020c). *On a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data (*C/2020/2296). Recuperado de https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf

COMISIÓN EUROPEA. (2020d). *Orientaciones sobre las aplicaciones móviles de apoyo a la lucha contra la pandemia de covid-19 en lo referente a la protección de datos (*2020/C 124 I/01). Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52020XC0417(08)

COMISIÓN EUROPEA. (2020e). *Una Estrategia Europea de Datos* (COM/2020/66). Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52020DC0066

COMITÉ EUROPEO DE PROTECCIÓN DE DATOS. (2020). *Statement on the processing of personal data in the context of the COVID-19 outbreak*. Recuperado de https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf

CONSEJO EUROPEO. (2020). *Joint statement of the Members of the European Concil*. Recuperado de https://www.consilium.europa.eu/media/43076/26-vc-euco-statement-en.pdf

COOKSON, C. (16 marzo 2020). UK's original coronavirus plan risked 'hundreds of thousands' dead. *Financial Times*. Recuperado de https://www.ft.com/content/249daf9a-67c3-11ea-800d-da70cff6e4d3

DALG, P. (17 abril 2020). Entrevista a Hans-Christian Boos. *Der Tagesspiegel.* Recuperado de https://www.tagesspiegel.de/wirtschaft/entwickler-der-neuen-corona-app-auch-alle-zufallskontakte-in-der-u-bahn-koennen-gewarnt-werden/25750350.html

DE LA CAL, L. (10 julio 2020). Tercera ola de coronavirus en Hong Kong: las escuelas vuelven a cerrar. *El Mundo*. Recuperado de https://www.elmundo.es/internacional/2020/07/10/5f0835cefdddff30808b46a4.html

EGLEN, S. (2020). *Codecheck certificate 2020-010*. doi:10.5281/zenodo.3865491

FERGUSON, N. (2020a). *COVID-19 CovidSim Model.* Recuperado de https://github.com/mrc-ide/covid-sim

FERGUSON, N. [neil_ferguson]. (22 de marzo 2020b). I wrote the code (thousand of lines of undocumented C) 13+ years ago to model flu pandemics [Tweet]. Recuperado de https://twitter.com/neil_ferguson/status/1241835454707699713

FERGUSON, N., LAYDON, D., NEDJATI GILANI, G., IMAI, N., AINSLIE, K., BAGUELIN, M. Y DIGHE, A. (2020c). Report 9: Impact of non-pharmaceutical interventions (NPIs) to reduce COVID19 mortality and healthcare demand. doi:10.25561/77482

FRAUNHOFER HEINTICH HERTZ INSTITUTE FOR TELECOMS. (2020). *Proximity tracing to manage the coronavirus pandemic: Fraunhofer proposes a German approach*. Recuperado de https://www.hhi.fraunhofer.de/en/press-media/news/2020/proximity-tracing-to-manage-the-coronavirus-pandemic-fraunhofer-proposes-a-german-approach.html

GABRIEL, J.X., DANCE Y VALENTINO-DEVRIES, J. (24 enero 2020). Have a Search Warrant for data? Google wants you to pay. *The New York Times*. Recuperado de https://www.nytimes.com/2020/01/24/technology/google-search-warrants-legal-fees.html

GALLAGHER, J. (17 marzo 2020). Coronavirus: UK changes course amid death toll fears. *BBC*. Recuperado de https://www.bbc.com/news/health-51915302

GINSBERG, J., MOHEBBI, M., PATEL, R., BRAMMER, L., SMOLINSKI, M. Y BRILLIANT, L. (2009). Detecting influenza epidemics using search engine query data. *Nature* 457**,** 1012–1014. doi:10.1038/nature07634

GOOGLE. (12 noviembre 2019). New insights into human mobility with privacy preserving aggregation [Entrada blog]. Recuperado de https://ai.googleblog.com/2019/11/new-insights-into-human-mobility-with.html

GOOGLE. (2020a). Información sobre las notificaciones de exposición. Recuperado de https://support.google.com/android/answer/9930236

GOOGLE. (10 abril 2020b). Android contact tracing API. Recuperado de https://blog.google/documents/55/Android_Contact_Tracing_API.pdf

GOOGLE. (10 abril 2020c). Apple and Google partner on COVID-19 contact tracing technology [Entrada blog]. Recuperado de https://blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology/

GOOGLE. (3 abril 2020d). Ayuda de informes de movilidad local. Recuperado de https://support.google.com/covid19-mobility/answer/9824897?hl=es

GOOGLE. (10 abril 2020f). Contact Tracing, Bluetooth specification. Recuperado de https://blog.google/documents/58/Contact_Tracing_-_Bluetooth_Specification_v1.1_RYGZbKW.pdf

GOOGLE. (3 abril 2020e). Helping public health officials combat COVID-19 [Entrada blog]. Recuperado de https://www.blog.google/technology/health/covid-19-community-mobility-reports

GOOGLE. (3 abril 2020g). Informes de movilidad local sobre el COVID-19]. Recuperado de https://www.google.com/covid19/mobility/

GOOGLE. (s.d). Informe de transparencia, solicitudes de información sobre usuarios en todo el mundo. Recuperado de https://transparencyreport.google.com/user-data/overview

GOOGLE. (10 abril 2020h). Privacy-safe contact tracing using Bluetooth Low Energy [Entrada blog]. Recuperado de https://blog.google/documents/57/Overview_of_COVID-19_Contact_Tracing_Using_BLE.pdf

GOOGLE. (2009). Google Flu Trends. Recuperado de https://www.google.org/flutrends/about/

HARVEY, D. (2004a). Bajo el dominio del capital. Dentro *de* El nuevo imperialismo (p. 80). Madrid: Akal.

HARVEY, D. (2004b). Los circuitos del capital. Dentro *de* El nuevo imperialismo (p. 93). Madrid: Akal.

HARVEY, D. (2004c). La acumulación por desposesión. Dentro *de* El nuevo imperialismo (p. 115). Madrid: Akal.

HELLEWELL, J., ABBOTT, S., GIMMA, A., BOSSE, N. I., JARVIS, C. I., RUSSELL, T. W., Y FLASCHE, S. (2020). Feasibility of controlling COVID-19 outbreaks by isolation of cases and contacts. *The Lancet Global Health*. doi: 10.1016/S2214-109X(20)30074-7

HINCH, R., PROBERT, W., NURTAY, A., KENDALL, M., WYMANT, C., HALL, M., Y FRASER, C. (abril 2020). Effective configurations of a digital contact tracing app: A report to NHSX. Recuperado de https://cdn.theconversation.com/static_files/files/1009/Report_-_Effective_App_Configurations.pdf?158753121

IPLYTICS. (2019). *Who is leading the 5G patent race?* (p.5). Recuperado de https://www.iplytics.com/wp-content/uploads/2019/01/Who-Leads-the-5G-Patent-Race_2019.pdf

KEELING, M. J., HOLLINGSWORTH, T. D., Y READ, J. M. (2020). The Efficacy of Contact Tracing for the Containment of the 2019 Novel Coronavirus (COVID-19). *medRxiv*. doi:10.1101/2020.02.14.20023036

KELION, L. (21 abril 2020). Coronavirus: Apple and France in stand-off over contact-tracing app. *BBC*. Recuperado de https://www.bbc.com/news/technology-52366129

LAZER, D., KENNEDY, R., KING, G., & VESPIGNANI, A. (2014). The Parable of Google Flu: Traps in Big Data Analysis. *Science*, *343*, 1203–1205. doi:10.1126/science.1248506

LOCKE, J. (2006). Segundo tratado sobre el gobierno civil. Madrid: Tecnos.

MACASKILL, E., Y DANCE, G. (1 noviembre 2013). NSA Files decoded. *The Guardian*. Recuperado de https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded

MÉNDEZ, M.A. (22 abril 2020). El alemán al que acusan de engañar a media Europa con 'apps' contra el coronavirus. *El Confidencial.* Recuperado de https://www.elconfidencial.com/tecnologia/2020-04-22/pepp-pt-hans-christian-boos-apps-coronavirus-covid19_2557724/

MINISTRY OF HEALTH AND WELFARE OF SOUTH KOREA. (2020). *Your information is our best defense against COVID-19*. Recuperado de https://www.mohw.go.kr/eng/nw/nw0102vw.jsp?PAR_MENU_ID=1007&MENU_ID=100703&page=1&CONT_SEQ=355356

MINISTRY OF HEALTH OF ISRAEL. (2020a). Hamagen. Recuperado de https://govextra.gov.il/ministry-of-health/hamagen-app/download-he/

MINISTRY OF HEALTH OF ISRAEL. (2020b). Hamagen, condiciones de uso. Recuperado de https://govextra.gov.il/ministry-of-health/hamagen-app/terms-and-conditions-of-use-en/

MINISTRY OF HEALTH OF SINGAPOR. (2020a). Bluetrace. Recuperado de https://bluetrace.io/

MINISTRY OF HEALTH OF SINGAPORE. (2020c). Tracetogether. Recuperado de https://www.tracetogether.gov.sg/

MORIN-DESAILLY, C. (20 marzo 2013). L'Union européenne, colonie du monde numérique? Informe en nombre de la comisión de asuntos europeos del Senado de Francia (nº 443). Recuperado de: https://www.senat.fr/rap/r12-443/r12-443_mono.html

NAKASHIMA, R. (14 agosto 2018). AP Exclusive: Google tracks your movements, like it or not. *Associated Press*. Recuperado de https://apnews.com/828aefab64d4411bac257a07c1af0ecb/AP-Exclusive:-Google-tracks-your-movements,-like-it-or-not

NATIONAL HEALTH COMMISSION OF THE PEOPLE'S REPUBLICO OF CHINA. (2020). *Health QR code helps curb the spread of COVID-19*. Recuperado de http://en.nhc.gov.cn/2020-03/28/c_78431.htm

NOAH HARARI, Y. (2019). La religión de los datos. Dentro de Homo Deus (p.400). Barcelona: Penguin Random House.

ORGANIZACIÓN MUNDIAL DE LA SALUD. (2017). *Contact traicing*. Recuperado de https://www.who.int/news-room/q-a-detail/contact-tracing

ORGANIZACIÓN MUNDIAL DE LA SALUD. (2020). *Rueda de prensa sobre la COVID-19 celebrada el 11 de marzo del 2020*. Recuperado de https://www.who.int/es/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020

PARK, S., CHOI, G.J., KO, H. (2020). Information Technology–Based Tracing Strategy in Response to COVID-19 in South Korea—Privacy Controversies. *JAMA.* 2020;323(21):2129–2130. doi:10.1001/jama.2020.6602

PARLAMENTO EUROPEO, COMISIÓN DE LIBERTADES CIVILES, JUSTICIA Y ASUNTOS DE INTERIOR. (12 marzo 2014). *Sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los Estados Unidos* (2013/2188(INI)). Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52014IP0230

PARLAMENTO EUROPEO. (17 abril 2020a). *EU coordinated action to combat the COVID-19 pandemic and its consequences* (2020/2616(RSP)). Recuperado de https://www.europarl.europa.eu/doceo/document/TA-9-2020-0054_EN.pdf

PARLAMENTO EUROPEO. (mayo 2020b). National COVID-19 contact traicing apps. Recuperado de https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/652711/IPOL_BRI(2020)652711_EN.pdf

PATERSON, K. [kennyog]. (16 de abril 2020). I'm really confused about what the @PeppPT approach to COVID-19 contact tracing really is. No details on their website, no public spec [Tweet]. Recuperado de https://twitter.com/kennyog/status/1250752812780343297

PENTLAND, A. (2015a). Social pressure. Dentro de Social physics (p.65). Nueva York: Penguin Books.

PENTLAND, A. (2015b). Visualizing the city. Dentro de Social physics (p. 140). Nueva York: Penguin Books.

PENTLAND, A. (2015c). What is social physics? Dentro de Social physics (p. 4). Nueva York: Penguin Books.

PEPP-PT. (1 abril 2020a). PEPP-PT web. Recuperado de https://web.archive.org/web/20200401105259/https://www.pepp-pt.org/

PEPP-PT. (10 abril 2020b). PEPP-PT web. Recuperado de https://web.archive.org/web/20200410043647/https://www.pepp-pt.org/

PEPP-PT. (16 abril 2020b). PEPP-PT web. Recuperado de https://web.archive.org/web/20200416081403/https://www.pepp-pt.org/

PÉREZ COLOMÉ, J. (16 abril 2020). La ingeniera española que lidera la 'app' europea de rastreo de contagios: "No será un estado de vigilancia". *El País*. Recuperado de https://elpais.com/tecnologia/2020-04-15/la-ingeniera-espanola-que-lidera-la-app-europea-de-rastreo-de-contagios-no-debe-ser-un-estado-de-vigilancia.html

REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS. (2016). Protección de datos desde el diseño y por defecto. Recuperado de https://gdprinfo.eu/es/es-article-25

SCIENTIFIC ADVISORY GROUP FOR EMERGENCIES. (2020a). *Coronavirus (COVID-19): scientific evidence supporting the UK government response*. Recuperado de https://www.gov.uk/government/news/coronavirus-covid-19-scientific-evidence-supporting-the-uk-government-response

SCIENTIFIC ADVISORY GROUP FOR EMERGENCIES. (2020b). *Measurement of effectiveness of risk mitigation measures in reducing transmission*. Recuperado de https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/905042/S0623_Measurement_of_effectiveness_of_risk_mitigation_measures_in_reducing_transmission.pdf

SIMONITE, T. (9 mayo 2017). Google's new Street View cameras will help algorithms index the real world. *Wired*. Recuperado de https://www.wired.com/story/googles-new-street-view-cameras-will-help-algorithms-index-the-real-world/

SMICHT, M. (4 abril 2020). Entrevista a Yuval Noah Harari. *XLSemanal*. Recuperado de https://www.xlsemanal.com/personajes/20200412/yuval-noah-harari-despues-coronavirus-mundo-crisis-historia.html

STATCOUNTER. (2020). *Mobile operating system market share Europe.* Recuperado de https://gs.statcounter.com/os-market-share/mobile/europe

STATUTES OF THE REPUBLICO OF KOREA. (2015). Infectious disease control and prevention act. Recuperado de https://elaw.klri.re.kr/eng_mobile/ganadaDetail.do?hseq=37239&type=abc&key=INFECTIOUS%20DISEASE%20CONTROL%20AND%20PREVENTION%20ACT&param=I

THE STATE COUNCIL OF THE PEOPLE'S REPUBLICO OF CHINA. (2020). *China introduces novel coronavirus close contact detection app*. Recuperado de http://english.www.gov.cn/2020special/5e32830ec6d019625c60433b/202002/10/content_WS5e40f488c6d0a585c76caf3a.html

TIDY, J. (17 marzo 2020). Coronavirus: Israel enables emergency spy powers. *BBC*. Recuperado de https://www.bbc.com/news/technology-51930681

TRONCOSO, C., PAYER, M. HUBAUX, J., SALATHÉ, M., LARUS, J., BUGNION, E., LUEKS, W., STADLER, T., PYRGELIS, A., ANTONIOLI, D., BARMAN, L., CHATEL, S., PATERSON, K., CAPKUN, S., BASIN, D., JACKSON, D., PRENEEL, B., SMART, N., SINGELEE, D. ABIDIN, A. SEDA, G., VEALE, M., CREMERS, C., BINNS, R. (2020). Decentralized Privacy-Preserving Proximity Tracing. Recuperado de https://github.com/DP-3T/documents/blob/deda384610587339f10aa0fe116c36896fb42d7d/DP3T%20White%20Paper.pdf

VELD, S. [SophieintVeld]. (17 de abril 2020). Who is PEPP-PT? A body setting standards for contact tracing apps must be fully transparent [Tweet]. Recuperado de: https://twitter.com/SophieintVeld/status/1251221787192578048

VICE. (10 abril 2020). *Shelter in place with Shane Smith & Edward Snowden* [Video]. YouTube. https://www.youtube.com/watch?v=k5OAjnveyJo

VINER, K. (2020). Entrevista a Naomi Klein. *elDiario.es*. Recuperado de https://www.eldiario.es/internacional/theguardian/naomi-klein-virus-obliga-pensar-relaciones-e-interdependencias-capitalismo-ensena-no-pensar_128_6101074.html

WANG, N., LI, Y., FAN, Z, MA, M., SHI, B., TIAN, W., XIA, Q., ZHANG, X., WU, Q., SUN, T., JIAO, M., SHAN, L. (2020). Comprehensive Community Epidemic Prevention and Control Models to Repel COVID-19 Pandemic-Grid-based management and digital response Experience from Four Provinces of China. doi: 10.2471/BLT.20.258053.

WAYMO. (s.d). FAQ. Recuperado de https://waymo.com/faq/

WIEWIÓROWSKI, W. (2020a). *EU Digital Solidarity: a call for a pan-European approach against the pandemic*. Recuperado de https://edps.europa.eu/sites/edp/files/publication/2020-04-06_eu_digital_solidarity_covid19_en.pdf

WIEWIÓROWSKI, W. (2020b). *Monitoring spred of COVID-19*. Recuperado de https://edps.europa.eu/sites/edp/files/publication/20-03-25_edps_comments_concerning_covid-19_monitoring_of_spread_en.pdf

WHITELAW, S., MAMAS, M. A., TOPOL, E., Y VAN SPALL, H. G. (2020). Applications of digital technology in COVID-19 pandemic planning and response. *The Lancet Digital Health*. doi: 10.1016/ S2589-7500(20)30142-4

WHITTAKER, Z Y ETHERINGTON, D. (13 de abril 2020). Q&A: Apple and Google discuss their coronavirus tracing efforts. *Techcrunch*. Recuperado de https://techcrunch.com/2020/04/13/apple-google-coronavirus-tracing/

WIKILEAKS. (29 junio 2015). *Espionnage Élysée.* Recuperado de https://wikileaks.org/nsa-france/

XNET. (1 junio 2020). Mas claridad sobre la utilidad de la inteligencia artificial (IA) y a los datos contra la propagación del COVID-19 desde la perspectiva de las libertades civiles. Recuperado de https://xnet-x.net/inteligencia-artificial-datos-covid19/

ZUBOFF, S. (2019a). Justice at the new frontier of power. Dentro de The Age of Surveillance Capitalism (p.480). Londres: Profile books.

ZUBOFF, S. (2019b). The secrets of extraction. Dentro de The Age of Surveillance Capitalism (p.87). Londres: Profile books.

ZUBOFF, S. (2019c). Two species of power. Dentro de The Age of Surveillance Capitalism (p.87). Londres: Profile books.