ieee.es
Instituto Español de Estudios Estratégicos
1970 — 2020

Documento
Opinión

36/2020 23 de abril de 2020

Lorenzo Cotino Hueso *

Inteligencia Artificial y vigilancia digital contra la COVID-19 y contra la privacidad. El diablo está en los detalles

Inteligencia Artificial y vigilancia digital contra la COVID-19 y contra la privacidad. El diablo está en los detalles

Resumen

De China no solo ha venido la COVID-19, sino el riesgo de la vigilancia digital masiva. La inteligencia artificial (IA) y el *big data* han fallado estrepitosamente. No obstante, serán esenciales en esta guerra contra el coronavirus en la investigación biomédica. Pero, con todas las garantías posibles y especialmente respecto del uso de las *apps*, geolocalización masiva y pasaportes biológicos que se van a ir desarrollando. Lejos de posiciones maximalistas, el diablo está en los detalles y nos va la vida en ello, no solo la privacidad ni la salud.

En este artículo se detalla cómo la iniciativa europea a la que se suma España está diseñada para evitar las tentaciones del diablo de acumular datos, de usarlos para otros fines y de evitar nuestro control.

Palabras clave

COVID-19, privacidad, Constitución, geolocalización.

Artificial Intelligence and digital surveillance against the Covid-19 and against privacy. The devil is in the details

Abstract

From China has come not only the COVID-19, but the risk of massive digital surveillance. AI and big data have failed spectacularly. However, they will be essential in this war against the coronavirus in biomedical research. But with all possible guarantees and especially regarding the use of apps, mass geolocation and biological passports. Far from maximalist positions, the devil is in the details and our lives are in it, not just privacy and health. It is described European initiative that Spain is joining. It is designed to avoid the temptations of the devil to accumulate data, to use it for other purposes and to avoid our control.

Keywords

Covid-19, privacy, Constitution, geolocation.

La inteligencia artificial y el *big data* han fallado estrepitosamente, pero serán esenciales en esta guerra contra el coronavirus

China exportó el coronavirus a todo el mundo. Ahora hay que desear que no exporte también su control social y vigilancia totalitaria. Como afirma Ferràs, parece que, frente al coronavirus, la D de la «disciplina» asiática ha sido mucho mejor que la «descoordinación» europea o el «darwinismo» norteamericano. Recuerda Han que la mentalidad autoritaria asiática y colectivista lleva a que no haya conciencia crítica ante la vigilancia digital y nos alerta de, que de la «psicopolítica» podemos pasar a la «biopolítica». En sentido similar, Harari nos previene de los peligros de una «vigilancia hipodérmica». Si el control «epidérmico» se «limitaba» a lo que tocábamos en la pantalla, ahora alcanza a nuestra temperatura, presión y muchos más datos para saber antes que nosotros si estamos enfermos, dónde hemos estado y con quién nos hemos reunido. Y que no se aproveche para muchas más finalidades.

Ahora bien, es muy importante no simplificar, polarizar y reducir la cuestión a una renuncia a la privacidad para mantener la vida o la salud, o para evitar los confinamientos y otras restricciones de nuestras libertades. Las lesiones de la privacidad, como el coronavirus, no se ven ni se sienten hasta que ya es tarde. Por ello, si se plantea el debate en estos términos maximalistas, nadie apostaría por la privacidad. El sistema democrático constitucional tiene bicentenaria experiencia para maximizar, balancear, armonizar y ponderar derechos fundamentales entre sí y con otros bienes constitucionales, a partir de una deliberación democrática cristalizada en la ley. La ética y el derecho pueden guiar soluciones tecnológicas para lograr maximizar la eficacia tecnológica contra el coronavirus minimizando los impactos en nuestros derechos. No es algo nuevo. Precisamente es toda la política y hoja de ruta de la IA basada en la ética y la privacidad en el diseño.

El *big data* y la IA han supuesto un rotundo fracaso en la prevención y alerta de la COVID-19, pero pueden ser muy útiles en la guerra contra el coronavirus e incluso para evitar confinamientos y otras restricciones de derechos que provoca. La IA va a ser extremadamente útil para integrar, estructurar y extraer información y conocimiento de ingente cantidad y variedad de *big data* en *datahubs*, «lagos de datos» o en *data warehouse*. Parte de estos datos proceden de los usos primarios de tratamientos médicos salud (análisis clínicos, imágenes, etc.). No obstante, cada vez más datos

resultan de usos secundarios de salud (aplicaciones, sensores, sistemas máquina a máquina o grandes transacciones de gestión de atención y facturación, biometría, redes sociales y aplicaciones). La mayoría son datos especialmente desestructurados que requieren de la IA para su ordenación, integración con otros y extracción de información, destacando la lectura natural de imágenes a partir del entrenamiento con sistemas de redes neuronales. Todo ello puede ser esencial para la investigación biomédica contra la COVID-19.

También la IA puede ser muy útil para la atención e información y prevención ciudadana, también con *chatbots*, mensajes perfilados e individualizados, para el autodiagnóstico. Asimismo, para la mejor prestación de los servicios de salud —y su descongestión— y la telemedicina. De igual modo, la IA puede ser muy útil para la mejor asignación de los recursos humanos y materiales en salud, tan necesarios. A su vez, a partir de estas interacciones masivas puede surgir muy valioso *big data* que retroalimente la investigación.

Una investigación con IA y datos masivos, pero con garantías

Este lado más amable del uso de la IA y el *big data* para la investigación biomédica es relativamente factible desde el punto de vista jurídico. Posiblemente, para que nadie les acuse de anteponer la vida y la salud a los datos, el Comité Europeo de Protección de Datos (EDPB, por sus siglas en inglés), el Supervisor Europeo (SEPD) y la Agencia Española (AEPD) o la catalana rápidamente han afirmado que «las reglas de protección de datos actualmente vigentes en Europa son lo suficientemente flexibles» (SEPD). Se ha dicho que el Reglamento Europeo de Protección de datos (RGPD) «permite a las autoridades de salud pública competentes y a los empleadores procesar datos personales en el contexto de una epidemia, de conformidad con la legislación nacional y en las condiciones establecidas en ella por parte de las autoridades públicas competentes» (EDPB)[1]. No obstante, jurídicamente hay muchos detalles por pulir, puesto que es precisa una legislación nacional que regule de modo más concreto esta

[1] EDPB. *Statement of the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak*. 20/3/2020. Disponible en https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en. Puede seguirse todos los documentos en el Observatorio, apartado «Privacidad». Disponible en https://www.uv.es/derechos/#_Toc38017389.

posibilidad y además hay que concretar exactamente qué se quiere hacer, quiénes y cómo. Para la investigación biomédica, la legislación actual puede considerarse que es suficiente. Ello es gracias a la reciente y muy positiva regulación de la LO 3/2018 de protección de datos (disposición adicional 17.ª). En todo caso, más allá de que no se requiera el consentimiento de las personas, siguen plenamente vigentes fuertes garantías de minimización de datos, estudios de impacto, seudonimización, deberes de confidencialidad de quienes los traten, participación de comités de ética y continua vigilancia de las autoridades. Hay que ser especialmente cautos para que nuestros «apetitosos» datos sensibles y los perfilados ni fluyan al sector privado ni sirvan para el control social «asiático».

Asimismo, no olvidemos que estos tratamientos automatizados y perfilados masivos de *big data* podrán acabar afectándonos individualmente. La IA puede acabar decidiendo nuestros tratamientos médicos y farmacológicos, entre otros muchos impactos en nuestros derechos. De ahí que de la mano del derecho respecto de decisiones automatizadas (art. 22 RGPD), serán necesarias especiales garantías de *white box* y transparencia de los algoritmos, frente a la opacidad natural de los sistemas de IA. Y habrá que garantizar siempre que la decisión última que nos afecte sea verdaderamente humana. Desde la Red de Derecho Administrativo de la Inteligencia Artificial (DAIA) hemos señalado no pocas de las garantías básicas que deben cumplirse[2].

Para quienes plantean los debates vida y salud contra privacidad, sería muy difícil que justificasen porqué los tratamientos de IA y *big data* en la lucha contra el coronavirus no pueden ser seguros, transparentes y controlables para que se ajusten a las finalidades que correspondan.

La mayor amenaza por el uso de *apps*, geolocalización masiva y pasaportes biológicos, mientras dure la guerra

Más amenazante, si cabe, para la privacidad puede ser el desarrollo de *apps,* pasaportes biológicos electrónicos, el uso masivo de sistemas de geolocalización, trazabilidad, metadatos y el rastreo monitoreo de toda la población como medida frente a la COVID-

[2] Ver las *Conclusiones de Toledo* de 1 de abril. Disponible en http://links.uv.es/PHAPt3I y la *Declaración final de Valencia* de 24 de octubre. Disponible en http://links.uv.es/e2w7MCR.

19, especialmente si se sigue el modelo asiático. En España, las comunidades autónomas en cascada han lanzado webs y aplicaciones, y el Gobierno encomendó a la Secretaría de Estado de Digitalización e Inteligencia Artificial (SGAD) una *app*, así como el cruce de datos estadístico con los operadores de telecomunicaciones a través del INE. Pocos días después, el SEPD apostó por una aplicación y respuesta cooperativa de la UE y, en esta línea, la SGAD ha sumado a España a la iniciativa *Pan-European Privacy-Preserving Proximity Tracing Project*. De momento, quizá solo se está dando un primer y relativamente tímido paso no comparable al modelo asiático. Pero no hay que excluir que se amplíen los usos y finalidades de esta u otras herramientas.

La misma semana de abril, Google y Apple han anunciado, de un lado, que integrarán sus sistemas operativos con los dispositivos para esas *apps* públicas. Pero, del otro lado, también anuncian que van a «habilitar una plataforma más amplia de rastreo de contactos basada en Bluetooth»[3], aunque no excluyen que se integre con otras aplicaciones. Muy posiblemente las grandes plataformas sabrán hacerlo «mejor» que el sector público, aunque no sabemos con qué riesgos añadidos a las aplicaciones públicas.

Jurídicamente, para permitir estos tratamientos más sensibles, el EDBP ha afirmado que —mientras dure la guerra— cabe aplicar la excepción de seguridad del artículo 15 Directiva 2002/58/CE de privacidad y comunicaciones. El mismo permite que la legislación española dé cobertura a estos tratamientos de datos más sensibles. Pero aquí las carencias de una ley española son mayúsculas y necesitamos más una regulación legal de calidad, claridad y con garantías. La STC 76/2019, de 22 de mayo declaró inconstitucional la ley que permitía a los partidos el perfilado político en las redes sociales, precisamente por no regular dicha ley las garantías precisas. Además, se requiere una ley no solo por exigencias «formales» de constitucionalistas, sino también democráticamente necesitamos la deliberación ética, política y social al respecto.

[3] Disponible en https://www.apple.com/es/newsroom/2020/04/apple-and-google-partner-on-Covid-19-contact-tracing-technology/.

Lejos de posiciones maximalistas, el diablo está en los detalles y nos va la vida en ello

De un lado, cabe qué fijar y para qué se van a utilizar estas aplicaciones y tratamientos masivos de datos. El impacto y las consiguientes garantías compensatorias puede variar mucho si con estas *apps* o sistemas se quiere facilitar una mera información ciudadana, o mejor asesoramiento, si son de autodiagnóstico, o llegan a servir para el tratamiento, diagnóstico y control médico y farmacológico. Estas *apps* o pasaportes biomédicos también pueden suponer barreras de acceso a servicios sociales, médicos, de transporte, pueden condicionar nuestra movilidad y circulación o el mismo acceso al trabajo y a establecimientos y actividades. Incluso pueden emplearse para el control administrativo, policial e incluso penal. En definitiva, pueden decidir nuestra vida. Además, no debe olvidarse que los datos masivos que se generan por estas *apps* y sistemas han de pasar a integrar el variado *big data* que es necesario reutilizar para investigar y controlar al coronavirus, no a las personas.

Otro detalle no poco importante es la voluntariedad de estas aplicaciones. De momento, en España y la UE (y el sistema PEPP-PT), así como Google y Apple, hablan de voluntariedad. Pero lo cierto es que jurídicamente el consentimiento, por lo general, no vale cuando se trata de los poderes públicos teniendo en cuenta el artículo 7. 4.º RPGD (Informe 185/2018 AEPD). Y, en ningún caso, sería un consentimiento válido si el uso de la *app* es condición para el acceso a zonas de la ciudad, transporte, servicios sociales, sanitarios, etc. Y siendo realistas, si estas aplicaciones son voluntarias y no se utilizan por casi toda la población, podrían llegar a ser inútiles para sus finalidades. De ahí la necesidad de legitimar legalmente su uso.

Los detalles de este «lucifer» no son solo relativos a qué se quiere hacer, también la clave es quién, cómo se hace y cómo controlarlo. La privacidad en el diseño, por defecto, será esencialmente relevante a la hora de configurar estos sistemas. Se trata de que estos sistemas y *apps* solo traten los datos exactamente para las finalidades concretas y no más. Igualmente, que se manejen los mínimos datos posibles necesarios. Es más, si son datos anónimos o lo más anónimos posible (seudonimizados) mucho mejor. Habrá de hacerse necesariamente una evaluación de impacto. De igual modo, la seguridad de la información será clave para evitar «*hackeos*» y fugas de tan sensible información debe darse incluso respecto de los datos anónimos, recuerda el SEPD. Cabe recordar que el

Libro blanco de la IA de la Comisión de la UE en febrero de 2020[4] ha abogado porque se implanten sistemas de control previo para tratamientos de IA de alto riesgo. La COVID-19 no va a dar tiempo a un testeo preventivo completo —aún no exigible— de estas *apps*. Pero la ciudadanía —en manos de especialistas— sí que ha de poder controlar estos sistemas y, especialmente, hay que reclamar que las autoridades de datos monitoreen continuamente su implantación y funcionamiento. Nos va la vida en ello.

A la iniciativa europea PEPP-PT, se ha sumado el Gobierno español y, en general, los países de la UE estos días, bajo el amparo de muchos científicos, universidades y empresas. Los detalles técnicos de la misma se detallan en un *Libro blanco* en constante actualización[5]. Ahí se señala cómo podría configurarse técnicamente una *app* o sistema de rastreo eficaz contra la COVID-19 en un buen equilibrio con la privacidad bajo el esencial principio de minimización y evitando que una entidad central acceda a los datos.

Se propone un sistema basado en teléfonos inteligentes para calcular localmente el riesgo de que un usuario individual haya contraído el virus en función de la exposición a personas infectadas. Un sistema para el rastreo de proximidad seguro que permita notificar a las personas que han estado en contacto con una persona infectada, sin revelar la identidad ni el lugar. No obstante, habrá que ver la potencialidad de ampliación para otros usos respecto de infectados, confinados, personas en cuarentena, etc.

Un diseño para evitar las tentaciones del diablo de acumular datos, de usarlos para otros fines y de que no lo podamos controlar

Un elemento esencial del sistema es que permite controlar los peligros de gran hermano. La iniciativa facilita productos bajo «código abierto», transparencia y auditable bajo licencia *opensource Mozilla*. El sistema además permite las diferentes implementaciones o *apps* nacionales, pero las mismas pueden ser interoperables entre los distintos países,

[4] Disponible en https://op.europa.eu/es/publication-detail/-/publication/aace9398-594d-11ea-8b81-01aa75ed71a1.
[5] AA. VV. *Decentralized Privacy-Preserving Proximity Tracing. White Paper*, versión 12/4/2020, en especial, 2020, pp. 2-3 y 29. Disponible en https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf.

algo esencial en la UE. El sistema afirma garantizar el RGPD y se certifica el cumplimiento de medidas de seguridad de modo auditable.

Bajo el principio de minimización y anonimización, se emplean identificaciones efímeras y pseudoaleatorias de los datos y movimientos de los cientos de millones de usuarios, los mismos solo se pueden utilizar una vez, la autoridad sanitaria declara que el usuario del sistema está infectado. Previamente a la declaración de infección, el sistema permite utilizar datos anónimos para calcular proximidad a infectados. Si la aplicación detecta un alto riesgo por un contacto, informará al usuario. Además, permite a los usuarios proporcionar voluntariamente información a los epidemiólogos para permitir estudios de la evolución de la enfermedad y ayudar a encontrar mejores políticas para prevenir futuras infecciones. Se puede compartir de manera voluntaria y privada datos sobre interacciones con personas infectadas (pero nunca contactan eventos en sí). Según afirman, el diseño descentralizado brinda a los usuarios un control detallado sobre la información que comparten y todo el intercambio de datos se realiza bajo el permiso explícito del usuario.

Asimismo, para evitar «tentaciones», resulta clave que el servidor central solo tenga identificadores anónimos de personas infectadas y, por su parte, los epidemiólogos obtienen la información mínima. Se evita un diseño central, esto es, *backend* que calcula los riesgos e informaría a los usuarios, pero que tendría el potencial de convertirse en infraestructura de vigilancia y control social. Por el contrario, desde PEPP-PT se «insta firmemente» a adoptar un sistema descentralizado. Los datos sobre situaciones de contacto específicos, es decir, las interacciones entre individuos siempre permanecen en los teléfonos de los usuarios y el cálculo del riesgo se realiza localmente, de acuerdo con las pautas establecidas por las autoridades de salud. De este modo, ninguna entidad puede abusar de los datos para otros fines, ni se puede conseguir que las otras entidades los faciliten. Y respecto de los no infectados, ninguna entidad puede acceder a sus identidades en función de identificadores efímeros emitidos.

Asimismo, destaca la idea de «desmantelamiento elegante» (*graceful dismantling*), puesto que, si no hay pacientes infectados, no se cargarán datos en el servidor y las personas dejarán de usar la aplicación. Asimismo, se prevé que los datos en el servidor se eliminen después de 14 días.

Esperemos que los desarrollos que sean necesarios y eficaces en esta situación excepcional sigan esta línea que combine eficacia, privacidad y transparencia. Y que no haya que acudir a desarrollos tecnológicos privados como los que anuncian Apple y Google. Los mismos, posiblemente garantizarán mejor la eficacia, pero muy dudosamente la privacidad y la transparencia.

*Lorenzo Cotino Hueso**
Catedrático de Derecho Constitucional Universidad de Valencia.
Coordinador Red www.derechotics, Observatorio Derecho Público y Constitucional y COVID-19 en España