Steven Forti

Francesca Bria: "La transición a la sociedad digital no puede basarse en un modelo securitario"

CTXT, 29 de abril de 2020.

En estas semanas se está hablando constantemente de aplicaciones para monitorear los contagios y evitar una nueva expansión de la covid-19. ¿Cómo funcionarían? ¿Respetarían la privacidad y las libertades fundamentales de los ciudadanos? ¿Existe el riesgo de perder el control sobre nuestros datos? ¿Estamos a las puertas de una sociedad de la vigilancia? Se trata de cuestiones muy complicadas que a menudo nos cuesta entender. Sin embargo, son temas fundamentales que atañen a nuestra vida y a nuestros derechos. Para conocer más sobre la tecnología aplicada al control de la pandemia y lo que están haciendo al respecto la Unión Europea y los diferentes Estados hablamos con Francesca Bria, una de las mayores expertas en temas de innovación digital en Europa. Actualmente es presidenta del *Italian Innovation Fund*, asesora de ONU-Habitat, el programa de Naciones Unidas para los Asentamientos Humanos, y profesora honoraria del *Institute for Innovation and Public Purpose*, dirigido por Mariana Mazzucato. Bria ha sido comisionada para Tecnología e Innovación Digital en el Ayuntamiento de Barcelona durante el primer mandato de Ada Colau, donde ha desarrollado proyectos a la vanguardia, como DECODE, para convertir los datos en un bien común. El año pasado se publicó en Italia su último libro *Ripensare la smart city*, escrito junto a Evgeny Morozov, uno de los intelectuales de referencia en el debate sobre los efectos sociales y políticos del desarrollo de las tecnologías.

Se habla mucho de aplicaciones para monitorear la situación sanitaria. ¿Qué se ha hecho hasta ahora en Europa?

La epidemia de covid-19 representa un reto sin precedentes para las democracias contemporáneas. Aunque el problema es global, la respuesta ha sido principalmente nacional, con una coordinación europea, y global a medida que pasaban las semanas. Siguiendo el ejemplo de países como Singapur, China y Corea del Sur, los gobiernos europeos han decidido apoyar los planes de la sanidad pública para contener el virus con la utilización de tecnologías y datos digitales. Las estrategias para la llamada "fase 2" incluyen una mezcla de acciones para controlar la tasa de mortalidad a través de medidas selectivas de confinamiento, test rigurosos y aplicaciones digitales para trazar los contactos y evaluar el impacto de las reaperturas selectivas en las áreas o sectores con más riesgos.

Según el estudio publicado por los científicos del Nuffield Department of Medicine de la Oxford University, el *contact tracing* (rastreo de contactos) es una medida fundamental. La aplicación será un soporte al *contact tracing* manual. Puede apoyarlo, pero nunca sustituir la profesionalidad del personal sanitario que debe tomar las últimas decisiones y comunicarlas con humanidad y competencia a las personas afectadas. Para ser eficaz, la aplicación deberá ser utilizada por una gran parte de la población, alrededor del 60%. Los efectos de la app deben comunicarse con transparencia: la tecnología debe ser segura y respetar los derechos y las libertades fundamentales de las personas. Solo así se podrá conquistar la confianza de los ciudadanos.

Para ser eficaz, la aplicación deberá ser utilizada por una gran parte de la población, alrededor del 60%

Muchos Estados de la UE han empezado a desarrollar aplicaciones para móviles utilizando enfoques y tecnologías distintas; se ha generado confusión y temor por la posible violación de la privacidad y las libertades fundamentales. Por eso, el Supervisor Europeo de Protección de Datos (SEPD) ha pedido que se adopte una solución paneuropea. La Comisión Europea ha presentado un plan de trabajo común para la contención del coronavirus que respete los principios establecidos por el organismo. El mismo Parlamento Europeo ha tomado una posición clara respecto de algunas condiciones clave de las tecnologías de trazabilidad de los contactos, pidiendo interoperabilidad a nivel europeo y respeto de los derechos fundamentales.

La UE había comenzado a trabajar en un sistema para la prevención de los contagios basado en el sistema abierto y en el pleno respeto de la privacidad. Sin embargo, parece que el proyecto se ha abandonado. ¿Por qué? ¿Qué pasó?

A principios de abril se creó un consorcio paneuropeo con ocho países y 130 investigadores llamado Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT). En un primer momento, en este consorcio existían enfoques distintos, pero había una voluntad común de desarrollar un sistema de *contact tracing* que tuviese como objetivo la privacidad y la protección de los datos de los ciudadanos. Sin embargo, las divergencias técnicas se convirtieron rápidamente en una verdadera batalla política sobre la dirección a seguir. En plena polémica, una parte de los académicos del consorcio decidió hacer pública la solución descentralizada que defendían y comunicaron el protocolo DP-3T, que había sido desarrollado por algunos de los mejores investigadores europeos sobre privacidad y ciberseguridad, entre los que se encuentra la española Carmela Troncoso.

¿Cómo funciona este protocolo DP-3T?

El almacenamiento de los datos está totalmente descentralizado. Es decir, los datos, protegidos con sistemas de anonimización o seudonominización, se conservan localmente en los dispositivos donde se hace también el cálculo del riesgo de infección. Si fuese necesaria la utilización de servidores centrales, deberán transmitirse solo unas claves anónimas y temporales correspondientes a los usuarios infectados, de manera que no sea posible conocer la identidad de las personas. La solución descentralizada responde perfectamente a la exigencia, propia de la normativa para la protección de los datos, de dejar a los ciudadanos el control sobre sus datos personales. Es un elemento fundamental que puede facilitar la confianza y la colaboración. Además, evita que toda autoridad, agencia o sujeto pueda utilizar de forma impropia los datos sanitarios que tienen un alto valor comercial y de inteligencia. Es lo que pide también el mismo Parlamento Europeo en una reciente resolución y los 500 firmantes de la carta abierta del Nexa Center for Internet and Society del Politecnico de Turín, entre los que aparecen los mayores expertos de tecnología y derecho italianos.

Una vez que un usuario haya señalado un síntoma o resultado positivo, la aplicación halla los contactos de los últimos siete días y avisa a los que se consideran de riesgo

Se habla mucho de trazabilidad a través de Bluetooth. ¿Qué significa?

La tecnología Bluetooth es menos invasiva y permite que los móviles de los usuarios detecten otros dispositivos cercanos sin la necesidad de registrar los datos sobre la posición de las personas. Cada vez que dos móviles se "encuentran", se intercambian su identificativo anónimo, utilizando el protocolo Bluetooth. Una vez que un usuario haya

señalado un síntoma o el resultado positivo del test, la aplicación halla los contactos más estrechos de los últimos siete días y avisa a los que se consideran de riesgo.

En una decisión sin precedentes, para hacer funcionar la tecnología Bluetooth garantizando la interoperabilidad de los dispositivos, Android e iPhone, Apple y Google han propuesto un enfoque común. El sistema, que estará listo en mayo y sobre el cual se apoyarán las aplicaciones nacionales que usarán Bluetooth, prevé que los datos de la lista de contactos entre los individuos, útiles para alertar sobre los que han estado cerca de algún positivo de covid-19, sean gestionados directamente por los móviles y no acaben en un servidor central gestionado por la administración pública. La propuesta de Apple y Google se coloca en la filosofía y los principios del modelo descentralizado inspirado por DP-3T al crear una API –es decir una interfaz de programación que permite a los programadores interactuar con la plataforma– a la cual las aplicaciones de los diferentes gobiernos se podrán conectar.

Varios gobiernos, como los de Francia, Alemania e Italia, han defendido un sistema centralizado con los datos de proximidad almacenados en un servidor central. Francia incluso ejerció presiones sobre Apple para eliminar las restricciones de Bluetooth en su app francesa, que se basa en un servidor central y una autoridad de confianza a nivel centralizado. Alemania ha cambiado finalmente de posición, adoptando la solución descentralizada, defendida por Suiza, Austria y Estonia. Italia y España, de momento, no tiene una postura clara al respecto y la decisión está aún en una fase de definición.

¿De quién tenemos que fiarnos? ¿De las multinacionales? ¿De los gobiernos? ¿De nadie?

Los investigadores europeos que propusieron una solución descentralizada han acogido con agrado la decisión de Google y Apple, pero piden auditorías externas para poder valorar la propuesta. No faltan también voces más críticas que alertan del aumento de poder de los gigantes de internet. Desde mi punto de vista, en este debate sería importante que la UE reconociera que los enfoques basados en descentralización y *privacy-by-design* no son opuestos a los esfuerzos europeos para recuperar soberanía tecnológica: al contrario, deberían representar la base para conseguir este objetivo. El hecho de que Google y Apple hayan decidido apostar por la solución lanzada por los mejores expertos europeos en el campo de la privacidad y la seguridad, adoptando la propuesta del proyecto europeo DP-3T, no constituye una amenaza para la soberanía europea, sino, más bien, la prueba de que los enfoques descentralizados y respetuosos de la privacidad y la protección de los datos de los ciudadanos funcionan. Europa debería estar orgullosa de esto.

¿Cómo se puede proteger al mismo tiempo salud y privacidad?

Creo que es importante no caer en la falsa dicotomía entre derecho a la privacidad y salud pública. Las tecnologías que se deben utilizar para la emergencia en un país democrático pueden y deben conjugar el objetivo de la seguridad sanitaria y la eficacia de la acción pública con la garantía de los derechos y las libertades fundamentales de las personas. El enfoque a seguir en Europa demuestra que es posible conjugar trazabilidad, eficacia y privacidad adoptando la tecnología Bluetooth, sin geolocalización, desarrollando una app con código abierto que puede ser auditada públicamente, con altos niveles de privacidad y estándares éticos y democráticos en relación al control de los datos personales. La descarga de la aplicación debe ser voluntaria y el protocolo utilizado debe incluir fuertes garantías de criptografía de los datos, descentralización de la arquitectura del sistema y anonimización,

haciendo prácticamente imposible conocer la identidad y los datos de las personas que utilizan los dispositivos. Esta solución ofrece a los individuos un mayor control del proceso y, al mismo tiempo, permite a los operadores sanitarios en el territorio trabajar de manera más rápida y eficaz. Es importante entender que la eficacia global de la solución no depende solo de la tecnología, sino del fortalecimiento del sistema territorial sanitario y de la cadena clínica: se debe aumentar el *contact tracing* manual tradicional, potenciar la capacidad de hacer test y tener una estrategia clara para la fase de recuperación.

En Italia se ha elegido una aplicación llamada Immuni [Inmunes], propuesta por una empresa de Milán, la Bending Spoon. ¿Cómo funciona?

Immuni será voluntaria, funcionará vía Bluetooth y se basará en código abierto. Los datos se borrarán y todo el sistema integrado de *contact tracing* lo gestionarán uno o más sujetos públicos que aún no se han definido. Todavía no está claro si la app italiana tendrá solo una funcionalidad de *contact tracing* o también un "diario sanitario": en este último caso habrá que explicar cómo funcionarán las otras herramientas sanitarias y cómo se integrarán con la aplicación de *contact tracing*. Italia tampoco ha aclarado si la app utilizará una arquitectura centralizada o descentralizada y qué protocolo adoptará. Son detalles técnicos importantes para entender bien el funcionamiento y analizar los riesgos.

Se ha lanzado también la propuesta de una especie de "pasaporte inmunitario". ¿Cómo funcionaría? ¿Qué implicaría?

Sobre el pasaporte inmunitario ya ha intervenido la OMS: no hay prueba alguna de que las personas que han estado contagiadas por covid-19 y luego se han recuperado sean inmunes a un segundo contagio, aunque tengan los anticuerpos. Esto debe desanimar a los gobiernos a introducir los "pasaportes inmunitarios" o las "certificaciones de riesgo cero".

En el caso de que no se apueste por este modelo democrático y respetuoso de la privacidad, ¿cuáles son los riesgos? ¿Qué perderíamos? ¿Iríamos hacia una sociedad de la vigilancia?

En general, esta crisis pone de manifiesto las decisiones existenciales que debemos encarar como sociedad frente a la digitalización. ¿Queremos un futuro orwelliano en que nuestros datos no son seguros y pueden ser manejados por gigantes digitales? ¿O queremos una sociedad digital más segura y justa en la que dispongamos de privacidad y tecnologías digitales que trabajen por el interés de los ciudadanos? Nos encontramos en un momento crucial en que se está acelerando la transición a la sociedad digital y no deberíamos adoptar un modelo basado solo en la emergencia y la seguridad. Lo que queremos evitar, por ejemplo, es que la preocupación del momento lleve a proponer o a adoptar leyes perjudiciales para la privacidad y la democracia. Deberíamos aprender de las experiencias del pasado y aprobar estas leyes después de un amplio debate que tenga en cuenta todos los elementos, a favor y en contra.

China ha utilizado los datos de los móviles para localizar a los millones de personas que dejaron Wuhan en las horas anteriores a la cuarentena

Algunos países han movilizado una amplia gama de instrumentos de vigilancia de masas, como app obligatorias que clasifican a las personas según el riesgo de contagio, *tracking* de masas y condivisión de informaciones personales y Big Data con las autoridades. China ha utilizado los datos de los móviles para localizar a los millones de personas que dejaron

Wuhan en las horas anteriores a la cuarentena; luego ha utilizado Alipay y WeChat HealthCode –una aplicación que colecciona los datos sanitarios y el historial médico– que generaban un código rojo, amarillo o verde para determinar la libertad de movimiento de las personas, dependiendo de si habían entrado en contacto con individuos contagiados. Singapur ha utilizado la aplicación Trace Together con un equipo de sanitarios para hacer investigaciones y entrevistas con el objetivo de localizar a los contagiados y planificar los test. Corea del Sur ha utilizado las correlaciones entre los datos de los móviles, los pagos con tarjetas de crédito y una app de trazabilidad basada en GPS para mapear los contagios.

La mayoría de las democracias occidentales rechaza justamente soluciones tan invasivas ya que harían aún más daño en el largo plazo. Los sistemas de vigilancia y perfilación de masas que permiten las tecnologías digitales generan fácilmente desigualdades y discriminaciones: sin adecuadas y estrechas garantías pueden socavar el ejercicio de todos los derechos de las personas. En otras palabras, el debate sobre la justa respuesta política y tecnológica a la covid-19 es solo un microcosmos del más grande dilema que las sociedades democráticas deben encarar: cómo amplificar la voz de los ciudadanos en la vida política sin frenar la innovación digital y parando las tentaciones populistas. Hay también un gran valor simbólico y geopolítico asociado a la resolución correcta de este problema. Ni el enfoque autoritario ni el americano liderado por las grandes tecnológicas son completamente compatibles con el respeto a los derechos humanos fundamentales que están en el centro del proyecto europeo. Si la UE no sabe resolver este problema, prestando especial atención y cuidado a las libertades civiles, eso comportará también la pérdida de una importante batalla internacional y geopolítica. Europa debería aprovechar este momento y demostrar que se puede ser innovador y al mismo tiempo introducir importantes tecnologías de las cuales depende el futuro de nuestra sociedad y nuestra economía. Ahora es el momento para demostrar que podemos hacerlo de forma distinta.

Usted ha sido comisionada a la innovación digital del Ayuntamiento de Barcelona en el primer mandato de Ada Colau y ha llevado adelante proyectos a la vanguardia en Europa. Defiende además otra idea de *smart city* según la cual los datos son un bien común y pertenecen a los ciudadanos.

Esta crisis podría acelerar la necesidad de proponer un nuevo pacto social sobre los datos. Está claro que organizar y recoger datos, analizarlos y utilizarlos para dirigir la acción pública es absolutamente fundamental para hacer frente a esta crisis que no es solo sanitaria, sino también económica, social y ambiental. Los datos se han convertido en un campo de batalla crucial en la guerra contra el coronavirus debido a que muchos países han utilizado métodos sofisticados para recoger y analizar los datos con el objetivo de monitorear y gestionar la pandemia.

Esto podría llevar a un cambio en el gobierno de los datos, abriendo el camino a un nuevo contrato social sobre la información personal y sus potenciales beneficios públicos. He trabajado sobre esto en los últimos años con el proyecto DECODE y con la propuesta de una nueva gestión de los datos como bien común en Barcelona. Hemos visto que la capacidad de utilizar datos y técnicas de inteligencia artificial para mejorar los servicios públicos puede dar resultados maravillosos. En general, necesitamos mayores inversiones en infraestructuras seguras para una utilización de los datos anónimos gestionados de manera ética y democrática.

En la economía digital los datos son material bruto y el corazón del modelo del *business* de las plataformas digitales es la extracción y la monetización de los datos personales. Hasta ahora la UE ha invertido demasiado poco en crear alternativas propias en la gestión de las infraestructuras críticas de la economía del futuro –cloud, datos, inteligencia artificial, supercomputing– y el sector público, con pocas excepciones, no ha articulado una verdadera estrategia. Pero muchas de las decisiones sobre los datos –tráfico, recogida de basura, limpieza de las calles, para no hablar de la actual ola de aplicaciones digitales en el ámbito de la medicina y la educación online– se pueden tomar utilizando los datos con total respeto de la privacidad. Tenemos también tecnologías emergentes descentralizadas como la *blockchain* y protocolos criptográficos, en los que Europa representa la excelencia, que permiten conjugar innovación y soberanía sobre los datos de los ciudadanos.

La utilización de los datos es de gran interés público. Sin embargo, para recuperar una gestión democrática de los datos y las infraestructuras digitales serán necesarias reglas fuertes para prevenir la consolidación de los monopolios, los abusos de poder y la creación de nuevos modelos de gobernanza o también nuevas instituciones como los "*data trust*" para repensar el modelo de control y propiedad, garantizar el reconocimiento del valor público de los datos y la redistribución de la riqueza producida.

En una crisis como esta se está viendo una profunda centralización de todas las decisiones, también en campo tecnológico. ¿Qué posibilidades tiene una opción democrática que desde abajo combine salud y respeto a los derechos?

Podemos construir una sociedad digital que respete los derechos, que sea innovadora y que permita a los ciudadanos tener voz sobre cómo se toman las decisiones en las infraestructuras digitales, que son infraestructuras estratégicas sobre las cuales basar los futuros modelos sociales y económicos. Para salir de esta crisis necesitaremos una agenda política ambiciosa que se haga cargo de la desastrosa situación económica y social, pero también adecuada para planear la transición digital y ecológica. No podemos superar esta fase con una política autoritaria post-democrática o tecnocrática. Necesitamos una fuerte implicación y la participación de la ciudadanía. La sociedad civil, los expertos de tecnología, los investigadores y los periodistas deben poder participar en el debate público para analizar el impacto de esta crisis y explicar a todos los ciudadanos las medidas y las políticas que se aplicarán, incluidas las determinantes decisiones tecnológicas. En el largo plazo, estoy convencida de que deberemos trabajar a partir de la red de ciudades para promover una política digital que ponga en el centro la participación de los ciudadanos y que esté al servicio de las soluciones de los grandes retos sociales y ambientales. Necesitamos una revolución tecnológica al servicio de la transición ecológica y debemos convertir la tecnología en un derecho y una oportunidad para muchos y no en un privilegio para pocos.

Steven Forti es profesor asociado en Historia Contemporánea en la Universitat Autònoma de Barcelona e investigador del Instituto de Historia Contemporánea de la Universidade Nova de Lisboa.