José Luis Carretero Miramar

Tecnología en tiempos de pandemia. La lucha por los datos

La epidemia de Covid 19 está poniendo en crisis gran parte de los paradigmas básicos de nuestra vida en sociedad. Como en una turbulenta reacción en cadena, el mundo está cambiando de manera radical. Nada será ya nunca más como antes.

España afronta la epidemia con un sistema sanitario degradado y al borde del colapso. Décadas de recortes, de cierres de centros de salud y de privatización y externalización de los servicios sanitarios o los servicios auxiliares de los hospitales, están pasando su factura. Cuando el brote de coronavirus comienza, el Sistema Público de Salud de la Comunidad de Madrid tiene cerca de dos mil camas hospitalarias y más de mil trabajadores sanitarios menos que diez años antes. Frente a las más de quinientas plazas en unidades de cuidados intensivos por cada cien mil habitantes de Alemania, la salud pública española no llega siquiera a las doscientas. Más de un treinta por ciento de los trabajadores de los servicios de salud son contratados temporales, muchos de ellos en claro fraude de ley.

Pero el caos en el sistema productivo es aún mayor. Las medidas de confinamiento y la consiguiente parálisis económica conllevan más de un millón de despidos. Los Expedientes de Regulación Temporal de Empleo (ERTEs) permiten suspender las relaciones laborales de más de cinco millones de trabajadores, que pasan a cobrar la prestación de desempleo. Los autónomos y las pequeñas empresas tienen que paralizar sus actividades y pasan a depender de las ayudas públicas. Los trabajadores informales (trabajadoras sexuales, trabajo sumergido en la hostelería o el turismo, operarios de pequeñas reformas en la edificación, vendedores ambulantes, etc.) y las personas que están en situación de marginalidad o sin hogar, tienen que recurrir a los Bancos de Alimentos de la Iglesia, los municipios o los movimientos sociales que, además, interrumpen en muchos casos su funcionamiento durante el plazo de confinamiento más estricto.

Los derechos y libertades reconocidos en la Constitución se ven limitados: el gobierno prohíbe las manifestaciones del primero de mayo, se imponen más de cien mil sanciones y se realizan miles de detenciones por la transgresión de las normas del confinamiento. A los detenidos, se les toma declaración mediante videoconferencia, sin la presencia física de su abogado en el lugar de detención. Las fuerzas de seguridad y el Ejército gozan de un enorme protagonismo público, mientras las metáforas sobre la "guerra contra el virus", "el campo de batalla" y "los soldados disciplinados" se vuelven omnipresentes en los medios de comunicación y en las ruedas de prensa de los representantes institucionales.

La tecnología ocupa el lugar de la sociabilidad y de los derechos ciudadanos. El teletrabajo se expande, sin que se respeten las normas legales que lo rigen (voluntariedad, derecho a la desconexión digital, control de la salud laboral, limitación de horarios, que las herramientas tecnológicas sean puestas a disposición del trabajador por el empresario y pagadas por él). Se repite el mantra del "distanciamiento social", que profundiza, por su propia condición de consigna innecesariamente extensiva y aberrante, la desarticulación comunitaria generada por las necesarias medidas de distanciamiento físico.

En este escenario convulso se plantea de manera cada vez más perentoria la necesidad de una solución tecnológica frente a la tempestad. Una nueva generación de herramientas, hijas de la técnica moderna, se nos dice, puede ser imprescindible para controlar la pandemia. Estamos hablando de los instrumentos que facilitan la toma de temperatura de los ciudadanos al entrar en las empresas o los comercios, de las apps de control del Covid-19, en sus diferentes modalidades, o, incluso, de la utilización de la tecnología para la realización de actividades de evaluación en el sistema educativo o para el nuevo teletrabajo.

Exámenes por Skype. Reuniones por Zoom. Pero también cámaras termográficas para medir la temperatura corporal en tiempo real, con mecanismos de Inteligencia Artificial que permiten detectar, además, si la persona que pasa lleva puesta una mascarilla.

Cámaras inteligentes como las fabricadas por la compañía china Dahua Technologies, que pueden registrar la temperatura corporal de todo el que entra en una tienda. Permiten detectar hasta a tres personas por segundo con una precisión de tres décimas de grado y a menos de tres metros de distancia. Desde que se instalaron en la ciudad de Wuhan, el pasado 24 de enero, Dahua ha vendido miles de estos dispositivos en toda China. Amazon le acaba de comprar 1.500, por un valor cercano a los diez millones de dólares. Cientos de ellas ya están instaladas en empresas españolas.

Las cámaras inteligentes toman la temperatura, pero tienen también instalado software que permite el reconocimiento facial, para identificar a los supuestos enfermos que pasen a su lado, o para ejercer el control del aforo limitado en un comercio. Éveris Aeroespacial, Defensa y Seguridad, ha adaptado tecnología que ya tiene instalada en el aeropuerto de Mallorca, que permite el embarque mediante identificación biométrica del pasajero, para que también tome su temperatura. La compañía gallega Beabloo ha preparado una herramienta digital basada en sensores e inteligencia artificial que permite determinar la posición de los clientes en una tienda y, después, avisar al responsable de que no se están guardando las distancias de seguridad.

Y junto a las cámaras, la geolocalización y las apps que la permiten. Apps de información voluntaria de contagios, como la desarrollada el inicio de la pandemia por la Comunidad de Madrid; apps de seguimiento de contactos por bluetooth, que permiten identificar a las personas que han estado cerca del propietario de un móvil que, posteriormente, resultan estar infectadas, como las que pretende implantar la Unión Europea, con el apoyo de Google y Apple. Y también, en última instancia, pasaportes de inmunidad mediante un código de colores o un código QR instalado en el propio smartphone, para que el vigilante de la empresa o institución que se quiere visitar pueda comprobar si se puede permitir o no el acceso al portador.

Máquinas, capacidad de computación, pero también su base fundamental de funcionamiento: datos. Los datos son el nuevo maná económico de la emergente Cuarta Revolución Industrial. Las Smart Cities del futuro próximo (ciudades inteligentes, donde todo está conectado, desde los semáforos y las cámaras de tráfico, hasta los historiales médicos o educativos de los ciuda-

danos) necesitan una cantidad ingente de datos y la capacidad de conectarlos y gestionarlos masivamente que van a asegurar las redes 5G y el Edge computing. Pero también los necesitan los nuevos modelos de negocio de los grandes "unicornios" (empresas que facturan más de 1.000 millones de dólares) de la tecnología.

Amazon, Facebook, Alphabet (la empresa matriz de Google) no serían nada sin los datos y sin la capacidad de computación y los nuevos avances en Inteligencia Artificial y en conectividad que permiten hacerlos operativos. Datos de nuestra navegación en las redes sociales, de nuestras búsquedas en internet, de nuestras compras con tarjeta. Datos de geolocalización que permiten saber dónde hemos estado y con quién (en eso se basan las apps propuestas para el control del Covid, pero también aplicaciones de citas o marketplaces virtuales que te presentan ofertas del restaurante más cercano en tu smartphone). Datos que permiten saber el interés que tenemos por acceder a un determinado servicio (hemos cargado tres veces la página pese a que no conseguimos entrar a la primera), cuánto tiempo pasamos navegando por una determinada web y en que páginas nos hemos detenido, qué es lo que compramos y cuánto gastamos en nuestra última visita a Amazon. Datos que permiten realizar ofertas, segmentar mercados, diseñar y probar modelos de negocio, determinar horarios (¿cuándo pasa más gente por esta calle?), personalizar la experiencia del cliente, conocer exhaustivamente los gustos, amistades, manías y costumbres de nuestros compradores y proveedores, saber, exactamente, de que pie virtual cojea un solicitante de un puesto de trabajo.

Los datos son el nuevo petróleo del siglo XXI. Todo el mundo quiere el acceso al Big Data, al control y tratamiento de los datos. Las grandes cantidades de datos dan una ventaja competitiva decisiva, en los mercados saturados de un capitalismo en crisis. Y, en los últimos diez años, se han desarrollado los avances cualitativos necesarios en la investigación en Inteligencia Artificial que permiten dar un salto de gigante en la automatización de la producción y en el manejo de los datos. Gracias a las técnicas de "aprendizaje profundo", los logaritmos de la IA actual, alimentados por una ingente cantidad de datos (cuántos más mejor) pueden empezar a aprender por sí mismos. A más datos, más aprendizaje, decisiones automatizadas más fundamentadas, mayor precisión, mayor probabilidad de acierto para el logaritmo y, a su vez… más y mejores datos y mayor aprendizaje.

Pero hay problemas importantes con los datos, con su uso social, con la mixtura creciente entre Inteligencia Artificial, Big Data y conectividad 5G. Uno de los grandes problemas tiene que ver con la geopolítica: ¿Quién tiene los datos? ¿Para qué los usa? ¿Qué importancia tiene eso en la dialéctica de los poderes en un mundo cada vez más multipolar? El segundo gran problema tiene que ver con la producción: si los datos llevan a la automatización, ¿qué ocurrirá con millones de puestos de trabajo que pueden ser automatizados? ¿De qué podemos vivir nosotros si muchas de las cosas que ahora hacemos pueden ser mejor realizadas por un algoritmo? Y el tercer gran problema, en el que nos vamos a detener en este texto por su estrecha relación con las propuestas de solución tecnológica a la pandemia de Covid-19: ¿Quién tiene el control de nuestros datos? ¿Qué van a hacer con ellos? ¿Pueden ser nuestros datos la herramienta de una nueva esclavitud y de un control autoritario de la sociedad sin paragón en la Historia de la Humanidad? ¿Qué tiene que ver eso con el Covid-19?

La cuestión geopolítica es clave para acceder al background intelectual que nos permita analizar el escenario en que nos encontramos: en estos momentos la lucha por el control del desarrollo tecnológico y económico del futuro es la lucha por los datos. Estados Unidos veta a Huawei, desata guerras comerciales contra China, impone sanciones a quienes ayuden a estructurar el sector tecnológico del gigante asiático.

Va a ser una guerra sin cuartel, porque en este momento, los chinos tienen una enorme ventaja en un aspecto decisivo: tienen más datos que nadie. Al respecto, nos limitaremos a citar un fragmento del libro "Superpotencias de la Inteligencia Artificial. China, Sillicon Valley y el Nuevo Orden Mundial", de Kai Fu-Lee, un ingeniero que ha trabajado en muchas de las más importantes empresas globales del sector:

"Hasta hace unos cinco años, tenía sentido comparar directamente el progreso de las compañías de internet chinas y estadounidenses en los términos de una competición (…) Pero hacia 2013, el internet de China dio un golpe de timón (…)

Los urbanitas chinos empezaron a pagar por comprar en el mundo real con códigos de barras en sus teléfonos, parte de una revolución de pagos móviles no vista en ningún otro lugar. Ejércitos de repartidores de comida y masajistas a la carta que se desplazaban en motos eléctricas obstruyeron las calles de las ciudades chinas. Representaban una onda sísmica de startups online-to-offline que llevaron las ventajas del comercio electrónico a los servicios del mundo real (…) La unión de todos estos servicios dio lugar a la aparición de la super app china We Chat, una especie de navaja digital del ejército suizo para la vida moderna. Los usuarios de We Chat empezaron a enviar mensajes de texto y de voz a sus amigos, a pagar sus compras, a pedir una cita con el médico, a pagar impuestos, a desbloquear bicicletas compartidas y a comprar billetes de avión, todo ello sin salir de la aplicación. We Chat se convirtió en la aplicación social universal, en la que se utilizaban diferentes tipos de grupos de chat -formados con compañeros de trabajo y amigos, o entorno a intereses concretos- para negociar acuerdos comerciales, organizar fiestas de cumpleaños o discutir sobre arte moderno. Reunió una serie de funciones esenciales que en Estados Unidos y otros países se encuentran dispersas en una docena de aplicaciones.

Ahora, el universo digital alternativo de China crea y captura un montón de nuevos datos sobre el mundo real. Esa riqueza de información sobre los usuarios -su ubicación cada segundo del día, qué alimentos les gustan, cuándo y dónde compran comida y cerveza- es valiosísima en la era de la implementación de la IA. Proporciona a estas empresas un pormenorizado tesoro de los hábitos diarios de estos usuarios, que puede combinarse con algoritmos de aprendizaje profundo para ofrecer servicios a medida que van desde la auditoría financiera hasta la planificación urbanística. También supera ampliamente lo que las compañías líderes de Sillicon Valley pueden descifrar a partir de tus búsquedas, "likes" u ocasionales compras online. Este incomparable tesoro de datos del mundo real dará a las empresas chinas una importante ventaja en el desarrollo de servicios basados en la inteligencia artificial."

Por supuesto, la preeminencia china en la acumulación de datos presupone un rasgo cultural y político previo: no hay límites reales a lo que puede ser acumulado. En China no hay una política pública de protección de los datos de los ciudadanos ni dicha protección se considera un derecho fundamental. Hay motivos culturales para ello (la cultura china siempre ha primado lo comunitario sobre lo individual y el tratamiento de los datos permite mejorar procesos, aunque exponga a los individuos a nuevos riesgos para su privacidad), pero también hay motivos propiamente políticos: si China se considera una nación socialista dirigida por la vanguardia del proletariado, constituida en Partido Comunista, no hay razón aparente para la opacidad de los individuos frente a las necesidades comunitarias expresadas coactivamente por el Estado y por las empresas. En Europa, sin embargo, sí tenemos, hoy en día, una legislación, imperfecta, pero al menos escrita y accesible, destinada a la protección de los datos personales. La privacidad es considerada un derecho fundamental del individuo. El origen histórico

que justifica esta legislación parece estar claro para los académicos del Derecho: el censo de la población alemana realizado por Hitler al inicio de su mandato, donde, por primera vez, se incorporó el dato del origen étnico de los ciudadanos, y que fue una herramienta imprescindible para la ejecución sistemática del Holocausto judío y el Samudaripen gitano. Una historia turbia que tuvo sus siniestras secuelas en suelo europeo: el censo de la población yugoslava realizado a la muerte de Tito, en el que, contra la dicción expresa de la Constitución de la República Federativa de Yugoslavia, se incorporó la "nacionalidad" étnica de los ciudadanos. Todos sabemos cómo acabó eso.

Así que tenemos que ser vigilantes con nuestros datos. Y aquí es donde volvemos a las apps del Covid y a la toma de temperatura en los lugares públicos. Porque al hablar de ello, no estamos hablando de otra cosa que de datos y, además, de datos especialmente sensibles por referirse a elementos centrales e íntimos de la propia personalidad (la salud, los datos biométricos que permiten el reconocimiento facial, etc.). Los medios de comunicación nos muestran las ventajas de la solución tecnológica al Covid. Los periódicos empresariales (Cinco Días, Expansión) publican cotidianas loas a la funcionalidad de las apps de control del virus y de los sistemas de control termográfico de los trabajadores. La Unión Europea avanza en el desarrollo de un sistema de aplicaciones para rastrear los contagios. Las autoridades alemanas han decidido adherirse al sistema implementado por Google y Apple, basado en el bluetooth, al que consideran más garantista de la privacidad que un sistema centralizado. Francia, España e Italia han apoyado al consorcio europeo PEPP-PT, impulsor de la app germana.

La propuesta de Google y Apple se basa en un sistema descentralizado. Los móviles de los usuarios intercambian un código cifrado y anonimizado por bluetooth con los smartphones cercanos. Si un usuario da positivo a Covid-19 e informa a través de la aplicación, los ciudadanos que hayan estado cerca de él en las últimas semanas recibirán una alerta. Esto evita, en principio, la existencia de un gran repositorio centralizado de datos, que pueda ser hackeado o utilizado para otros usos.

Sin embargo, esto puede no ser suficiente para garantizar los derechos ciudadanos. Un informe de mayo de 2020 de la Agencia Española de Protección de Datos (una entidad pública de control que difícilmente puede ser calificada de "conspiranoica" o "anticapitalista"), titulado "El uso de las tecnologías en la lucha contra el Covid19. Un análisis de costes y beneficios" nos indica que:

"Las principales amenazas a la privacidad de este tipo de soluciones vienen de la realización de mapas de relaciones entre personas, re-identificación por localización implícita, de la fragilidad de los protocolos a la hora de construir "tarjetas" casi anónimas, y de dispersar las señales de los contagios de forma que no se identifique en ningún caso la identidad de los contagiados. Debe de tenerse en cuenta que el tratamiento de la información no afecta sólo al usuario de la aplicación, sino también a todos los terceros con los que ha estado en contacto (…)

Hay estudios sobre la robustez de los protocolos de criptografía y anonimización, y siempre existe una posibilidad de que, aplicando suficiente tiempo y capacidad de cómputo pueden romperse y asociar los apodos anónimos con números de teléfono y personas."

Hemos de señalar que, a este respecto, la capacidad de intervención de los programadores de Apple o Google sobre los cerrojos criptográficos de los datos es, simplemente, de un orden inmensamente superior a cualquier cosa que puedan hacer nuestros técnicos del sistema público de tecnología.

¿Representan los datos recogidos en estas aplicaciones un beneficio sanitario importante en la crisis provocada por la pandemia? La Agencia Española de Protección

de Datos también nos responde, tentativamente, a este interrogante:

"Una vez más, es necesario poner de manifiesto que las soluciones técnicas no se pueden considerar de forma aislada. El éxito de este tipo de soluciones se basa en muchos factores que no dependen de la tecnología. En primer lugar, es necesaria la implicación de un número elevado de usuarios, algunos estudios hablan de al menos el 60% de una población que, teniendo en cuenta a los niños y los ancianos, suponen casi todos los usuarios de móvil. Por otro lado, depende de que se realice una declaración responsable de la situación personal de infección, preferiblemente supervisada por un profesional para evitar estrategias de desinformación. Finalmente, es necesario disponer de acceso a test, no sólo para todos los usuarios, sino para poder actualizar la información periódicamente y para que aquellos que sean notificados de haber estado en contacto con un infectado puedan realizar la prueba con prontitud".

Respecto a los famosos "pasaportes de inmunidad", muy divulgados por ciertos sectores empresariales que ya los están implantando en sus centros de trabajo, el mismo documento de la AEPD nos informa de que:

"Estas aplicaciones móviles están anticipando lo que puede ser un futuro documento de identidad en el móvil, con el riesgo añadido de incluir y mostrar un dato de salud, e incluyendo todos los riesgos que se derivan de las vulnerabilidades de dichos sistemas: acceso a manos de ciberdelincuentes, cruce con otros datos como la localización, incorporación de metadatos, lectura remota o, simplemente, no estar al alcance de muchas personas que no pueden usar teléfonos inteligentes."

Sin embargo, el instrumento tecnológico más utilizado en estos momentos no son las distintas apps, ni los pasaportes de inmunidad, sino las cámaras termográficas con reconocimiento facial, que permiten prohibir el acceso a una persona con una temperatura corporal alta a un centro de trabajo o comercio. El 30 de abril de 2020, la Agencia Española de Protección de Datos hace público un comunicado respecto al uso de estos dispositivos en comercios, centros de trabajo y otros establecimientos.

La AEPD empieza por darnos una información sanitaria básica, pero que tiende a ser olvidada en los debates mediáticos sobre este asunto: uno puede tener una temperatura alta y no tener el Covid (por tener un flemón, por ejemplo) y, también puede tener una temperatura baja y estar infectado por el coronavirus (ser asintomático).

La Agencia, entonces, "se muestra preocupada, por este tipo de actuaciones, que se están realizando sin el criterio previo y necesario de las autoridades sanitarias". Es más, la AEPD nos informa de que:

"Este tratamiento de toma de temperatura supone una injerencia particularmente intensa en los derechos de los afectados. Por una parte, porque afecta a datos relativos a la salud de las personas, no sólo porque el valor de la temperatura corporal es un dato de salud en sí mismo sino también porque, a partir de él, se asume que una persona padece o no una concreta enfermedad, como es, en estos casos, la infección por coronavirus.

Por otro lado, los controles de temperatura se van a llevar a cabo con frecuencia en espacios públicos, de forma que una eventual denegación de acceso a un centro educativo, laboral o comercial estaría desvelando a terceros que no tienen ninguna justificación para conocerlo que la persona afectada tiene una temperatura por encima de lo que se considere no relevante y, sobre todo, que puede hacer sido contagiada por el virus.

En último extremo, y dependiendo del contexto en que se aplique esta medida, las consecuencias de una posible denegación de acceso pueden tener un importante impacto para la persona afectada."

Tenemos que ser conscientes de que determinados datos son considerados como especialmente sensibles (los datos biométricos, los relativos al estado de salud, la

afiliación sindical y política…). ¿Pueden tratarlos personas sin ninguna formación para ello, como el tendero de la esquina y que, además, lo hacen sin responder ante ninguna autoridad legal concreta? ¿Le daríamos pruebas de nuestra orientación sexual al recepcionista del gimnasio para que las incorporara a un fichero de la empresa, en un ordenador conectado a internet? ¿Dejaríamos escanear nuestro carnet sindical, con todos los datos relativos a nuestra dirección y edad, a la puerta del supermercado de nuestro barrio?

La crisis del Covid-19 tiene un inevitable e innegable aroma distópico. Pero no olvidemos que la crudeza de la situación tiene más que ver con la degradación del sistema público de salud por las políticas de austeridad y la consiguiente falta de recursos, que con diatribas sobre la "irresponsabilidad" y la "culpa" de nuestros vecinos. El problema de fondo es que la Sanidad pública puede colapsar porque ha sido abandonada y desmantelada en las últimas décadas. Otra cuestión a tener en cuenta es que, aunque la legislación europea obliga a destruir los datos tras su uso legítimo, nadie controla que empresas, gobiernos o grupos de interés, hagan realmente eso. Incluso es casi imposible, desde el punto de vista técnico, asegurarse de que se ha hecho.

Los datos son el petróleo del siglo XXI. Pero es un petróleo que está hecho de nuestros gustos más personales, nuestra intimidad más profunda, los elementos más únicos de nuestra personalidad irrepetible, nuestras vergüenzas, nuestros miedos y todo aquello que puede ser usado contra nosotros por una autoridad fuera de control. Se está gestando el Gran Censo de todos nuestros datos, y la pandemia puede acelerar ese proceso. Datos que se venden, que se hackean, que pueden ser un arma peligrosísima en las manos equivocadas. Nos hemos convertido en "vida puesta a trabajar" hasta en nuestras elecciones más íntimas, hasta en los accidentes biológicos de nuestro devenir. La democracia de los datos, el común de los datos que respete, también, la individualidad inalienable de cada uno de nosotros y nuestros ámbitos de privacidad, está aún por construir.