La protección de datos en la lucha contra el coronavirus

Este artículo aclara el rol de la protección de datos en situaciones de crisis para la seguridad: no opuesto a la salud o la vida, sino compatible y garantizando el bienestar y el respeto a los derechos y libertades fundamentales.

Son múltiples los desarrollos tecnológicos que se han promovido por distintos países y organizaciones para luchar, de un modo u otro, contra la pandemia del coronavirus SARS-CoV-2. En España también han surgido varias iniciativas, desde webs, aplicaciones, estudios de movilidad, uso de *chatbots* e incluso algunos medios hablan de una reciente propuesta de utilización de *blockchain* para la trazabilidad de los contagios[1].

Estos proyectos han suscitado ciertas inquietudes por los posibles tratamientos de datos personales que pueden conllevar y han surgido voces recordando que, por mucha emergencia en que estemos inmersos, debe seguir respetándose el derecho a la protección de datos. Con ello la polémica queda servida: ¿datos versus vida? ¿Privacidad contra innovación? ¿Protección de datos por encima de la salud?

Este tipo de dicotomías, como la que surgió en EE. UU. tras los atentados terroristas del 11-S (seguridad vs. privacidad), parten de una concepción errónea de lo que es el derecho a la protección de los datos personales[2]. Lo que la normativa en esta materia protege no son los datos, sino lo que hay detrás de ellos: las personas.

La normativa europea de protección de datos no obstaculiza estos desarrollos tecnológicos, sino que sienta las bases para que, aprovechando todos sus beneficios para combatir la epidemia, los derechos y libertades fundamentales de los individuos no resulten perjudicados de forma injustificada o abusiva.

Los Considerandos del Reglamento General de Protección de Datos nos dan las pautas para interpretar su propio articulado. Resulta esclarecedor, en este sentido y en relación con el tema que tratamos, leer con atención algunos de dichos Considerandos, como el segundo de ellos cuando indica que el Reglamento "pretende contribuir a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas".

Por su parte, el Considerando 4 comienza diciendo que el tratamiento de datos personales "debe estar concebido para servir a la humanidad" y el 46 prevé que algunos tratamientos respondan "tanto a motivos importantes de interés público como a los intereses vitales del interesado, como por ejemplo cuando el tratamiento es necesario para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria".

La protección de datos no supone en modo alguno un impedimento para el superior derecho a la vida y a la salud

En conclusión, la protección de datos no supone en modo alguno un impedimento para el superior derecho a la vida y a la salud. Por el contrario, sin apartar el foco de ese bien superior, ofrece las garantías para evitar que el resto de derechos de los individuos se vean menoscabados o para que, de ser necesario que alguno de tales derechos ceda, lo haga en la justa medida que efectivamente resulte necesario y no de un modo arbitrario o desproporcionado.

Como decimos, son muchos los proyectos que se han creado y se están creando, con base tecnológica, bien para analizar cómo se comporta el virus, bien para la realización de autoevaluaciones sobre COVID-19, bien para poder ofrecer información y descongestionar así las vías de atención telefónica de los organismos públicos que se han visto desbordadas, etcétera.

En relación con las webs y aplicaciones de evaluación y/o información, es posible que, conforme estén diseñadas y las finalidades concretas que se persiga con ellas, no precisen realmente el tratamiento de datos personales, más allá de aquellos que puedan necesitar recabar por razones técnicas (como el tipo de dispositivo utilizado, su sistema operativo, etcétera). Sin embargo, en caso de que sí se traten datos personales y sean relativos a la salud de personas individualizadas o individualizables, debe tenerse en cuenta que, con carácter general se requerirá el consentimiento explícito e informado del usuario, salvo que la web o aplicación sea responsabilidad de un organismo o administración pública con competencias en el ámbito de la salud pública, en cuyo caso el tratamiento de los datos también podrá estar basado en el interés público.

En lo que respecta a los estudios de movilidad, normalmente estos se realizan obteniendo un gran volumen de información de distintas fuentes, fundamentalmente operadores de telefonía -que son quienes poseen datos masivos de esta naturaleza- que se traslada ya al responsable del tratamiento de manera anonimizada y agregada. Esto significa que previamente, las entidades en posesión de la información “original” la procesan para eliminar los datos personales -los que puedan identificar a la persona a la que pertenecen o hacerla identificable- y luego la agrupan por distintos rangos, tales como código postal o localidades, sexo, franjas de edades, etcétera, según resulte compatible con el objetivo del estudio.

Se intenta garantizar que la información quede totalmente anonimizada, pero cada vez es más difícil garantizar la anonimidad al cien por cien

De esta forma se intenta garantizar que la información quede totalmente anonimizada, de modo que ya no

haya datos de carácter personal y no le sea aplicable a esa información la normativa sobre protección de datos. Sin embargo, debe tenerse en cuenta que cada vez es más difícil garantizar la anonimidad al cien por cien. Pensemos, por ejemplo, en pequeñísimas localidades con muy escasa población en las que bien pudiera existir solo cuatro adolescentes entre los diez y los 15 años, perteneciendo tres de ellos a un mismo sexo y el cuarto a otro. Es presumible que las compañías telefónicas tienen gran cuidado en realizar sus procesos de anonimización de modo tal que no se produzcan situaciones de reidentificación. Pero en muchas ocasiones luego esa información bien anonimizada se cruza con otra procedente de otras bases de datos elaboradas en atención a otros criterios. Esa combinación puede acabar arrojando resultados en los que aflora la reidentificación de algunos de los registros.

Por tal motivo, conviene que los responsables de estos estudios de movilidad exijan contractualmente a sus proveedores, tanto compañías telefónicas como otros posibles, que realicen sus procesos de anonimización y, en su caso, de combinación de datos, de modo tal que se garantice que no podrá identificarse de manera individualizada a ninguna de las personas a quienes pertenecía en origen la información. Conviene igualmente, y por la misma razón, que, a pesar de encontrase anonimizados, se aplique a esos datos iguales o similares garantías y medidas de seguridad que merecerían en caso de ser datos personales.

Consideración distinta merece la introducción de *blockchain* en la trazabilidad de los contagios y cualquier otra fórmula que pueda derivar en una especie de etiquetado de las personas entre inmunes, contagiados activos y no contagiados. Un escenario como este merece sesudas reflexiones y análisis sumamente detallados en los que se incluya la anticipación de posibles situaciones y de potenciales usos por distintos agentes.

Se habla de los beneficios de este tipo de control exhaustivo para evitar la propagación de la pandemia, así como de poder contar con los inmunes para ir reactivando la economía. Pero algo así merece el máximo y más exquisito de los cuidados pues conllevaría, cuanto menos, que el concreto etiquetado de las personas fuera accesible por parte de algunas entidades. Basta pensar mínimamente cómo podrían pretender utilizar algunas compañías esa información (entidades financieras, compañías aseguradoras, las propias empresas respecto a sus empleados…), o cómo podríamos reaccionar los particulares en ciertas situaciones al cruzarnos con un contagiado activo, para imaginar lo fácil que sería pasar de una pandemia a una pandemia aderezada con su propia distopía. Fíjense, pues, si es o no útil y beneficiosa la protección de datos.

En cualquier caso, ante las suspicacias que cualquiera de las tecnologías que hemos comentado pueda generar, uno de los instrumentos que más confianza puede aportar a la ciudadanía es la publicación de las oportunas evaluaciones de impacto, ya sean sobre protección de datos, respecto de las tecnologías involucradas, o las relativas al impacto ético que puedan conllevar estos proyectos.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). *Diario Oficial de la Unión Europea*, de 4 de mayo de 2016. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *Boletín Oficial del Estado*, núm. 294, de 6 de diciembre de 2018. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673&p=20181206&tn=1

Narayanan, A. y Shmatikov, V. «Privacy and Security. Myths and Fallacies of 'Personally Identifiable Information'» en *Communications of the ACM,* Vol. 53, núm. 6, pp. 24–26, 2010.

Ohm, P. «Broken promises of privacy: Responding to the surprising failure of anonymization» en *UCLA Law*

Review, 57, pp. 1701–1777, 2010.

Wright, D. y De Hert, P. (2012). *Privacy Impact Assessment*. London/New York, Springer Science+Business Media B.V.

Wright, D. y Friedewald, M. «Integrating privacy and ethical impact assessments» en *Science and Public Policy* 40, pp. 755–766, 2013.