LOS TRATAMIENTOS DE DATOS PERSONALES EN LA CRISIS DEL COVID-19. UN ENFOQUE DESDE LA SALUD PÚBLICA.

Ricard Martínez Martínez

Director de la Cátedra de privacidad y Transformación Digital Microsoft-Universitat de Valencia

Diario La Ley, Nº 9601, Sección Doctrina, 25 de Marzo de 2020, **Wolters Kluwer**
Normativa comentada

Resumen
La crisis del COVID-19 nos enfrenta a un proceso de investigación clínica acelerada que ha planteado dudas sobre la posibilidad de tratar datos personales de los ciudadanos. Este trabajo trata de acreditar que la limitación del derecho fundamental a la protección de datos para el tratamiento de datos personales, de datos de salud y de datos de localización con fines epidemiológicos encontraría su fundamento en la protección de intereses vitales del interesado o de otra persona física (art. 6.2.c) RGPD, en un deber de colaboración de las operadoras basado en la seguridad pública, y en la competencia de las autoridades al amparo del artículo tercero de la Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública para «adoptar las medidas oportunas para el control de los enfermos».

En mi opinión ha llegado el tiempo del "cómo", y autoridades y expertos podemos y debemos contribuir en el esfuerzo. Este trabajo trata de acreditar que existen bases jurídicas razonables para todos los posibles tratamientos. Y también de desterrar temores infundados. Las autoridades sanitarias actúan con pleno sometimiento al Derecho y bajo el control de una autoridad independiente, cuando no de la justicia. Y necesitan a unos expertos en protección de datos que salgan de su confortable zona de campeones del no, y desplieguen una enorme vocación de servicio, de dedicación a la comunidad como aliados en la guerra contra la enfermedad.

La pandemia provocada por el patógeno COVID-19 ha puesto sobre la mesa las virtudes y carencias del modelo europeo de protección de datos personales. Este modelo se caracteriza por ofrecer un marco altamente tuitivo en la garantía del derecho fundamental a la protección de datos, particularmente funcional para la garantía de este derecho, pero también por un planteamiento proactivo que implica un compromiso de responsables y encargados en la garantía del derecho fundamental. Este modelo aporta sin duda enormes ventajas desde el punto de vista de la garantía de nuestras libertades en una sociedad democrática. Pero no está exento de inconvenientes cuando su aplicación no se modula desde un enfoque funcional. Y la crisis de COVID-19 ha puesto de manifiesto la existencia

de enfoques puramente reactivos, centrados exclusivamente en un enfoque desde el Reglamento General de Protección de Datos (LA LEY 6637/2016), con una interpretación del entero ordenamiento jurídico a la luz del derecho a la protección de datos. No son buenas noticias.

El Ordenamiento sitúa a las autoridades de protección de datos en una posición constitucional de significativa preeminencia y de juez último en muchos conflictos. Y esto puede producir un efecto paralizante poco conveniente en momentos en los que la protección del derecho fundamental a la vida y a la salud adquieren una relevancia primordial.

Esta situación de facto, que no *de iure*, implica una alta dependencia de todos los sectores respecto de los criterios que eventualmente fije el regulador caso por caso. Y la experiencia demuestra, al menos en nuestro país, algunas pautas que se vienen repitiendo de modo reiterado:

- **1.** Las autoridades de control son reactivas. Esto es, responden a consultas específicas, o conflictos concretos. En raras ocasiones abordan cuestiones generales salvo en *guidelines*.
- **2.** Cuando se definen criterios en sus guías —-elaboradas ya sea mediante recursos propios, ya mediante el recurso a la subcontratación de expertos--, no existe una consulta o debate público en la conformación de sus criterios. Esto afecta seriamente tanto a la calidad del resultado como la viabilidad de la implementación de recomendaciones muchas veces alejadas de la realidad material.
- **3.** El enfoque del regulador casi siempre opera desde el derecho fundamental a la protección de datos a la realidad, y casi nunca a la inversa. Y ello, no significa tan solo que se pierdan de vista elementos cruciales en los tratamientos de datos personales, sino también que se obvie en más de una ocasión la necesaria ponderación de derechos.

El resultado práctico no es otro que convertir la práctica en protección de datos en lo que mis colegas investigadores denominan un «guía-burros». Esto implica, que en la mayor parte de los casos los operadores se preocupen sobre cómo hacer las cosas según los criterios del regulador, y en escasas ocasiones se centren en cómo hacer las cosas del mejor modo posible.

I. *LA REALIDAD DE LOS HECHOS*

Desde un punto de vista material, las necesidades de procesar datos en el ámbito de la salud se han multiplicado exponencialmente. En el ámbito de la salud pública una de las cuestiones más polémicas es la que atiende a la localización de pacientes. Esta técnica presentaría usos muy diversos:

- ▪ La trazabilidad casi inmediata de las personas con las que se ha relacionado un paciente. En estos momentos, las herramientas con las que cuentan los servicios de Salud Pública para la localización de pacientes resultan en la práctica muy limitadas y con una secuencia temporal lenta y laboriosa.
- ▪ La asignación estratégica de medios y recursos. Operar con mapas que asignen dónde se encuentran enfermos que necesiten atención domiciliaria, o potencialmente hospitalizables, puede contribuir a una gestión dinámica de recursos humanos, asignación de hospitales e incluso a la identificación de necesidades materiales y gestión de stocks.
- ▪ En modelos experimentales se examina cómo la trazabilidad en el propio hospital puede incrementar la eficiencia y acelerar las condiciones de atención temprana.

Existen otras necesidades cuya solución dependerá del tratamiento de datos personales
Pero existen otras necesidades cuya solución dependerá del tratamiento de datos personales, y del uso de la analítica de datos y de la inteligencia artificial. Se trata de servicios destinados a resolver problemas como, por ejemplo:

- ▪ Saturación de líneas de atención.
    - **a.** En este sentido resulta posible definir criterios de asignación de un determinado valor de riesgo a una llamada mediante el cruce de datos sobre el origen de la llamada y los mapas de riesgos o mapas de infección que se hayan generado.
    - **b.** El uso de chatbots sirve para atender al ciudadano y no saturar líneas de atención o 112, cuando se trata de casos leves o dudas principalmente. Pero el análisis de las conversaciones puede ofrecer una analítica de las emociones que asista al gestor de la llamada tanto en el modo de atención como en la identificación de riesgos no revelados por personas cuyas capacidades se encuentren limitadas.
    - **c.** Habilitar teleconsultas permite que médicos y sanitarios en cuarentena que no pueden atender pacientes presencialmente, lo hagan telemáticamente y sirve, como están demostrando algunos modelos, para liberar recursos atendiendo las patologías más leves.

- ▪ Análisis de pacientes infectados y hospitalizados
    - **a.** El uso de Historias Clínicas Electrónicas para el seguimiento de pacientes, con técnicas de analítica de datos y metodologías decisionales basadas en inteligencia artificial ayudará hoy o en el futuro a identificar correlaciones relevantes y tomar decisiones sustentadas en datos. Pero ello implica el análisis de un lenguaje muy codificado, como el de la asignación de fármacos, junto con los

elementos propios del lenguaje natural presentes en una historia clínica.
- **b.** Emplear redes neuronales para detectar coronavirus en imágenes en radiografías y TACS. Las redes neuronales requieren de entrenamiento con los datos que se vayan generando.

Sea hoy o en el futuro, el estudio de aspectos como la comorbilidad, o la genética implican la necesidad de procesar historias clínicas de miles de personas. Finalmente, desde la experiencia investigadora puede intuirse la relevancia para el estudio retrospectivo de datos como por ejemplo los de carácter socioeconómico. Y no sólo esto, va a resultar imprescindible la generación de grandes lagos transnacionales de datos de salud anonimizados y de una intensa colaboración público-privada.

II. *UNA CUESTIÓN DE PONDERACIÓN DE DERECHOS*

Resulta por tanto necesario ponderar el potencial impacto en los derechos que garantizan la vida privada de las personas, y otros instrumentalmente relacionados, con los fines que persigue el derecho a la protección de la salud, incluida la salud pública del artículo 43 de la Constitución Española (LA LEY 2500/1978). Debe señalarse que en un contexto pandémico, el derecho a la protección de la salud, como principio rector de la política social y económica, cumple una función instrumental crucial en relación con la dignidad humana (artículo 10 CE (LA LEY 2500/1978)) y los derechos a la vida del artículo 15 (LA LEY 2500/1978), y a la seguridad (artículo 17 (LA LEY 2500/1978)) en la medida, en este último caso, en el que la salud pública adquiere un valor esencial para la garantía del orden público y la convivencia democrática.

Con carácter previo, no puede descontextualizarse este trabajo de un elemento subjetivo crucial: el juicio de proporcionalidad aplicado por el autor parte de una precondición axiológica previa que consiste en afirmar que toda vida humana es preciosa en sí misma. A partir de esta premisa, el juicio de ponderación constitucional que se llevará a cabo en cada escenario requiere considerar ciertos aspectos esenciales:

a. Los derechos fundamentales no se configuran como derechos ilimitados.

En expresión de nuestro Tribunal Constitucional:
«de una parte, que sólo ante los límites que la propia Constitución expresamente imponga al definir cada derecho o ante los que de manera mediata o indirecta de la misma se infieran al resultar justificados por la necesidad de preservar otros derechos constitucionalmente protegidos, puedan ceder los derechos fundamentales (SSTC 11/1981 (LA LEY 6328-JF/0000), fundamento jurídico 7.º; 2/1982 (LA LEY 16/1982), fundamento jurídico 5.º, 110/1984 (LA LEY 353-

TC/1985), fundamento jurídico 5.º), y de otra que, en todo caso, las limitaciones que se establezcan no pueden obstruir el derecho "más allá de lo razonable" (STC 53/1986 (LA LEY 10987-JF/0000), fundamento jurídico 3.º), de modo que todo acto o resolución que limite derechos fundamentales ha de asegurar que las medidas limitadoras sean "necesarias para conseguir el fin perseguido" (SSTC 62/1982 (LA LEY 7232-JF/0000), fundamento jurídico 5.º; 13/1985 (LA LEY 9639-JF/0000), fundamento jurídico 2.º) y ha de atender a la "proporcionalidad entre el sacrificio del derecho y la situación en que se halla aquel a quien se le impone" (STC 37/1989 (LA LEY 116723-NS/0000), fundamento jurídico 7.º) y, en todo caso, respetar su cometido esencial (SSTC 11/1981 (LA LEY 6328-JF/0000), fundamento jurídico 10; 196/1987 (LA LEY 903-TC/1988). fundamentos jurídicos 4.º, 5.º y 6.º; 197/1987 (LA LEY 98030-NS/0000), fundamento jurídico 11), si tal derecho aún puede ejercerse» (STC 120/1990 (LA LEY 1761-JF/0000)).»

b. La técnica de ponderación debe analizar la injerencia en el derecho a la vida privada desde un juicio basado en la idoneidad y la necesidad de la medida, regido por el principio de mínima intervención.

El Tribunal Europeo de Derechos Humanos ha afrontado la aplicación del artículo 8 CEDH (LA LEY 16/1950) desarrollando un método interpretativo que se articula en tres etapas de análisis netamente diferenciadas. En primer lugar, se trata de determinar si realmente se ha producido una injerencia en el derecho al respeto de la vida privada para, a continuación, verificar si dicha intromisión se halla prevista por ley y si es legítima y necesaria de acuerdo con las excepciones del párrafo segundo.

En esta primera fase la Corte no prejuzga en absoluto la licitud de la medida, únicamente constata si se trata o no de un supuesto que interfiere o vulnera el bien jurídico protegido por el precepto. La segunda y tercera secuencia del análisis se basan en el contraste del caso con lo dispuesto por el segundo párrafo del precepto. Una vez superado el *test* de legalidad, el Tribunal Europeo de Derechos Humanos finaliza su análisis emitiendo un juicio de proporcionalidad al amparo del principio de necesidad de la medida en una sociedad democrática. Desde el punto de vista de los límites admisibles al derecho a la vida privada, debe señalarse que existen un conjunto de principios comunes en distintos textos internacionales.

Así, el artículo 8.2 Convenio Europeo de Derechos Humanos (LA LEY 16/1950) incluye a la protección de la salud como fundamento para la limitación de aquel derecho.

La Carta de los Derechos Fundamentales de la Unión Europea reconoce el derecho a la protección de la salud en el artículo 35.

La Carta de los Derechos Fundamentales de la Unión Europea reconoce el derecho a la protección de la salud en el artículo 35. (LA LEY 12415/2007) Asimismo, contiene las previsiones relativas a las técnicas admisibles de limitación de los derechos fundamentales que no solo recogen la técnica del Convenio Europeo de Derechos, sino que directamente ordenan su aplicación en el párrafo tercero que dispone:
«(…)

3. En la medida en que la presente Carta contenga derechos que correspondan a derechos garantizados por el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (LA LEY 16/1950), su sentido y alcance serán iguales a los que les confiere dicho Convenio. Esta disposición no obstará a que el Derecho de la Unión conceda una protección más extensa.»

Así pues, cabe considerar que la protección de la salud constituye un valor que en el contexto del Convenio y la Carta puede limitar los derechos relacionados con la vida privada y al que nuestra Constitución confiere un valor constitucional significativo.

En el ámbito específico de la protección de datos personales el 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 (RGPD) ha reconocido idénticos valores en su Considerando (46) (LA LEY 6637/2016)
«(46) El tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física. En principio, los datos personales únicamente deben tratarse sobre la base del interés vital de otra persona física cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente. Ciertos tipos de tratamiento pueden responder 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, sobre todo en caso de catástrofes naturales o de origen humano.»

El criterio interpretativo que deriva del mismo resulta evidente: los tratamientos vinculados al control y lucha contra una epidemia encuentran cláusulas habilitantes cuando están en juego los intereses vitales de la comunidad.

1. *Las condiciones de predeterminación normativa*
En nuestro sistema constitucional la predeterminación normativa a la que se refiere el Tribunal Europeo de Derechos Humanos viene delimitada por la reserva de ley del artículo 53.1 CE. (LA LEY 2500/1978) En virtud de ello las

limitaciones a los derechos del artículo 18 de la Constitución Española (LA LEY 2500/1978) requieren de una norma con rango de ley, que en todo caso deberá respetar su contenido esencial.

Por otra parte, debe delimitarse el tipo de ley ya que ésta, en los términos del artículo 81 CE (LA LEY 2500/1978), deberá ser orgánica cuando implique un desarrollo de los derechos fundamentales. Por otra parte, el artículo 86 CE (LA LEY 2500/1978) excluye la posibilidad de los decretos-leyes cuando afecten al contenido esencial de tales derechos. Esto no implica, que otras normas jurídicas no puedan incidir en los derechos fundamentales. Sin embargo, esto plantea una restricción de orden práctico.

Para el despliegue rápido de cualquier acción que implique tratamiento de datos personales vinculados o no a la salud, será necesario delimitar si existe una reserva de Ley Orgánica en la medida en la que la limitación de los derechos del artículo comporte una afectación al contenido esencial del derecho fundamental a la protección de datos definido por la STC 292/2000 (LA LEY 11336/2000):

«7. De todo lo dicho resulta que el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.

En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también

a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele.»

2. *Principio de primacía y excepciones a los derechos en el Reglamento General de Protección de Datos*

El legislador europeo ha apostado por un Reglamento General de Protección de Datos (LA LEY 6637/2016). El principio de primacía de la norma europea, si bien con cierto margen de apreciación, asegura una garantía homogénea del derecho fundamental a la protección de datos funcional a las necesidades del Mercado Interior. En este sentido, cabe considerar al Reglamento como fuente de Derecho a la hora de identificar excepciones a las facultades que integran el contenido esencial de este derecho fundamental: esto es, la necesidad de consentimiento salvo excepción legal y los derechos de acceso, rectificación, supresión, portabilidad, limitación u oposición al tratamiento. Se aplicarían, por tanto, las excepciones previstas para el tratamiento de datos personales distintos de los datos de salud en el artículo 6.2, párrafos c), d, y e) RGPD (LA LEY 6637/2016) e:«c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física
e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento»

Y las previstas para el tratamiento de salud en el artículo 9.2, párrafos c), g), h) e i) (LA LEY 6637/2016).
«c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;
(…)
g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;
h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;
i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para

la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional»

Desde el punto de vista de la legislación nacional el fundamento para el tratamiento de datos personales sin consentimiento podría derivar de lo dispuesto en:

- ▪ El artículo 26 de la Ley 14/1986, de 25 de abril, General de Sanidad (LA LEY 1038/1986), por el que se atribuye competencias a los servicios sanitarios ante la existencia de un riesgo inminente y extraordinario para la salud, en los siguientes términos.
- ▪ La Ley Orgánica 3/1986, de 14 de abril (LA LEY 924/1986), de Medidas Especiales en Materia de Salud Pública (modificada mediante Real Decreto-ley 6/2020, de 10 de marzo (LA LEY 3058/2020), por el que se adoptan determinadas medidas urgentes en el ámbito económico y para la protección de la salud pública, publicado en el Boletín Oficial del Estado de 11 de marzo de 2020) que habilita para el control de los enfermos.
- ▪ La Ley 33/2011, de 4 de octubre, General de Salud Pública, amén de garantizar el derecho fundamental a la protección de datos en su artículo 9 (LA LEY 18750/2011), establece el deber de todas las personas de comunicar datos o circunstancias que pudieran constituir un riesgo o peligro grave para la salud. La colaboración con los servicios competentes resulta esencial para el logro de los objetivos que del Real Decreto 2210/1995, de 28 de diciembre (LA LEY 282/1996), por el que se crea la red nacional de vigilancia epidemiológica. Por otra parte, si COVID 19 es una variante de SARS (en español: Síndrome Respiratorio Agudo Grave), figura entre las enfermedades de declaración obligatoria del ANEXO I del Real Decreto 2210/1995, de 28 de diciembre (LA LEY 282/1996), por el que se crea la red nacional de vigilancia epidemiológica.
- ▪ El párrafo segundo apartado c) de la disposición adicional decimoséptima sobre tratamientos de datos de salud de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LA LEY 19303/2018), habilita al uso de datos con fines de investigación en salud pública sin consentimiento en circunstancias como una epidemia.

Una interpretación sistemática de la normativa sobre protección de datos personales habilitaría en consecuencia, a todos aquellos tratamientos que resulten necesarios para conseguir los objetivos de salud pública. Y así lo ha señalado la AEPD en su informe N/REF: 0017/2020, de 12 de marzo.

III. *LA REACCIÓN DE LAS AUTORIDADES DE PROTECCIÓN DE DATOS*

Si consideramos caso por caso, la reacción de las autoridades de protección de datos responde al patrón que señalábamos al principio y se ha centrado esencialmente en dos estrategias. La primera, resolver problemas o dudas concretas. La segunda, en su tarea de *enforcement*, esto es en evitar tratamientos abusivos de los datos personales al calor de la histeria colectiva. Es decir, en una actitud que viene siendo tradicional, sólo se ha respondido a preguntas del tipo «qué se puede hacer», «para qué se pueden usar los datos» y «quien los puede procesar». Pero no han respondido a la cuestión fundamental: «**¿cómo hacerlo?**»

Usemos un ejemplo tomado de Corea del Sur (Pueyo, 2020) (1) . En este país, los primeros treinta casos de coronavirus fueron controlados pero el paciente 31 resultó ser un súper-diseminador que lo contagió a miles de personas. En España, en la Unión Europea, en un caso similar ¿hubiéramos podido realizar un mapa temprano de estos miles de casos con referencia a personas identificadas? Es más ¿habríamos podido practicar *test* a cada potencial infectado usando unidades móviles mediante citas concertadas? La reciente respuesta del presidente del Comité Europeo de Protección de Datos que ha señalado en nota de prensa es negativa:

«Cuando se trate procesar no sólo datos anónimos, el art. 15 de la Directiva sobre la privacidad y las comunicaciones electrónicas (LA LEY 9590/2002) permite a los Estados miembros introducir medidas legislativas en pro de la seguridad nacional y la seguridad pública. Esta legislación de emergencia es posible a condición de que constituya una medida necesaria, apropiada y proporcionada dentro de una sociedad democrática. Si se introducen esas medidas, el Estado Miembro está obligado a establecer las salvaguardias adecuadas, como la concesión a las personas del derecho a un recurso judicial (2) .»

Sin embargo, cabe entender que en virtud de lo dispuesto en su Ordenamiento, para el Information Commissioner Británico existe una mayor flexibilidad (3) :

«We all share the same concerns about the spread of the COVID-19 virus. The need for public bodies and health practitioners to be able to communicate directly with people when dealing with this type of health emergency has never been greater.

Data protection and electronic communication laws do not *stop* Government, the NHS or any other health professionals from sending public health messages to people, either by phone, text or email as these messages are not direct marketing. Nor does it *stop* them using the latest technology to facilitate safe and speedy consultations and diagnoses. Public bodies may require additional collection and sharing of personal data to protect against serious threats to public health.

The ICO is a reasonable and pragmatic regulator, one that does not operate in isolation from matters of serious public concern. Regarding compliance with data protection, we will take into account the compelling public interest in the current health emergency.

The safety and security of the public remains our primary concern. The ICO and our colleagues in the public sector have this at the forefront of our minds at this time. We are here to help our colleagues on the frontline. We can offer advice to make sure the law around data protection and direct marketing is clear. Information is available on our website or you can call our helpline on 0303 123 1113.»

Sin perjuicio de nuestra extrañeza ante dos ejemplos tan rotundamente diversos los hechos son muy tozudos y demuestran algo muy evidente. Casi todos los pronunciamientos que ha venido indexando Padín (4) se pronuncian sobre aspectos específicos y con un enfoque reactivo.

Y este hecho, debe ser valorado antes por el ciudadano que por el jurista. Las autoridades de protección de datos están al servicio de la ciudadanía y deben rendir cuentas. Resulta sencillamente inadmisible que 28 autoridades y centenares de funcionarios, sin contar con el talento jurídico en cada territorio, hayan sido incapaces de desarrollar un esfuerzo concertado que proporcionase el adecuado fundamento para la actuación de los servicios de salud y la investigación sanitaria. Para un enfoque que atienda al valor constitucional de la dignidad humana frente al derecho a la salud y a la vida, nada puede prevalecer, porque, sin ellas, el propio derecho fundamental a la protección de datos carece de sentido.

IV. *LA CONSIDERACIÓN DE LOS METADATOS GENERADOS POR LAS COMUNICACIONES: LA GEOLOCALIZACIÓN*

Si atendemos a la posición manifestada por la presidenta del EDPB, el tratamiento de datos de salud para la investigación y su uso en condiciones de urgencia están avalados por el RGPD. Sin embargo, procesar metadatos de comunicaciones presenta serios problemas de protección de datos. Y por ello debe merecer una atención preferente en este trabajo, aunque no exclusiva. Anteriormente se ha señalado cómo la localización de un teléfono móvil puede resultar particularmente relevante desde el punto de vista del despliegue de las políticas públicas asociadas a la lucha contra COVID-19, ya sea para la localización y atención de enfermos, ya sea para la trazabilidad de estos y la prevención de posibles contagios o de la propia epidemia, en este caso mediante datos anonimizados.

En principio, esta materia se encuentra regulada en la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). Su artículo 2 (LA LEY 9590/2002)define dos conceptos relevantes:

«b) "datos de tráfico": cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma;
c) "datos de localización": cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público»

Desde el punto de vista de su definición, podría considerarse que no afectaría al derecho fundamental al secreto de las comunicaciones el uso de los datos de localización con fines epidemiológicos, cuando se trate de establecer la ubicación de un sujeto y de las personas con las que potencialmente se ha relacionado y a las que haya podido contagiar.

La Directiva sobre la privacidad y las comunicaciones electrónicas en su artículo 9 (LA LEY 9590/2002), regula el tratamiento de datos de localización distintos de los del tráfico restrictivamente, de modo que «sólo podrán tratarse estos datos si se hacen anónimos, o previo consentimiento de los usuarios o abonados, en la medida y por el tiempo necesarios para la prestación de un servicio con valor añadido». No obstante, el artículo 15 (LA LEY 9590/2002)de la norma establece ciertas excepciones cuando se trate de «una medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas». Este precepto ha sido interpretado a su vez por el Tribunal de Justicia de la Unión Europea en la sentencia (LA LEY 180541/2016) dictada en los asuntos acumulados C 203/15 y C 698/15, en los siguientes términos:

«90 (…) Dicha enumeración de objetivos tiene carácter exhaustivo, como se deriva del artículo 15, apartado 1, segunda frase, de esta última Directiva, a cuyo tenor las medidas legales deben estar justificadas por alguno de «los motivos establecidos» en el artículo 15, apartado 1, primera frase, de dicha Directiva. Por tanto, los Estados miembros no podrán adoptar tales medidas con fines distintos de los enumerados en esta última disposición.

91 (…) El artículo 15, apartado 1, de la Directiva 2002/58 (LA LEY 9590/2002) debe, por tanto, interpretarse a la luz de los derechos fundamentales garantizados por la Carta (véanse, por analogía, por lo que se refiere a la Directiva

95/46 (LA LEY 5793/1995), las sentencias de 20 de mayo de 2003 (LA LEY 2680/2003), Österreichischer Rundfunk y otros, C 465/00, C 138/01 y C 139/01, EU:C:2003:294, apartado 68; de 13 de mayo de 2014 (LA LEY 51150/2014), Google Spain y Google, C 131/12, EU:C:2014:317, apartado 68, y de 6 de octubre de 2015 (LA LEY 133806/2015), Schrems, C 362/14, EU:C:2015:650 (LA LEY 133806/2015), apartado 38).»

La sentencia citada plantea sin duda un interrogante: ¿Es posible una interpretación conforme a la Carta de los Derechos Fundamentales de la Unión Europea? Si el artículo 52 permite la limitación del derecho fundamental a la protección de datos en los términos del artículo 8.2 CEDH (LA LEY 16/1950) cuando respete el contenido esencial de dichos derechos y libertades ¿cabe un entendimiento del tratamiento de los datos de localización con fines de salud pública como un tratamiento instrumental al derecho a la vida?

En tal caso, cabe considerar la posibilidad de construir un enfoque de la cuestión en el que:

- ▪ El fundamento para el tratamiento de datos de localización se base precisamente en la presencia de un interés vital del paciente y de cualquier otra persona física. Su finalidad última, y la única admisible, no sería otra que la localización de todos los posibles sujetos contagiados, y en último extremo la ubicación del paciente tanto para evitar nuevos contagios como para asegurar una intervención rápida de los servicios de urgencias.
- ▪ Las garantías apropiadas derivarían obviamente del hecho que la actividad de los servicios de salud pública posee unas competencias muy claramente definidas en materia epidemiológica, y tanto la legislación general como la específica, garantizan el deber de secreto, el uso legítimo de los datos, y la seguridad de la información. En esta última materia, el Real Decreto 3/2010, de 8 de enero (LA LEY 630/2010), por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica provee de un estándar particularmente exigente.

En conclusión, la limitación del derecho fundamental a la protección de datos para el tratamiento de datos personales, de datos de salud y de datos de localización con fines epidemiológicos encontraría su fundamento en la protección de intereses vitales del interesado o de otra persona física (art. 6.2.c) RGPD (LA LEY 6637/2016), en un deber de colaboración de las operadoras basado en la seguridad pública, y en la competencia de las autoridades al amparo del artículo tercero de la Ley Orgánica 3/1986, de 14 de abril (LA LEY 924/1986), de Medidas Especiales en Materia de Salud Pública para «adoptar las medidas oportunas para el control de los enfermos».

V. *INTERROGANTES PARA EL FUTURO*

Si bien la cuestión de la localización ha monopolizado, por su sensibilidad y actualidad, parte de este trabajo, el resto de los usos potenciales de los datos presenta aristas que deberán ser tenidas en cuenta. Es evidente que el RGPD, y en particular el principio de la protección de datos desde el diseño y por defecto, abren un camino altamente feraz a la investigación científica y a la atención de los pacientes. Y en el caso español, la disposición adicional decimoséptima sobre tratamientos de datos de salud de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LA LEY 19303/2018) constituye una base sólida desde la que construir.

Durante años, las normas sobre protección de datos personales fueron interpretadas por muchos profesionales desde lo que un colega denomina muy afortunadamente la regla del «no». En alguna medida, esta cultura de la negación y de la subordinación de cualquier valor a la normativa sobre protección de datos personales ha producido un efecto de autorrestricción en el ámbito de la salud. A ello ayudaban criterios como por ejemplo el de considerar poco menos que imposible el uso compatible de los datos con fines de investigación. No es ocioso recordar cómo una cuestión de reputación asociada a la privacidad llevó al fracaso el ambicioso proyecto de Big Data de la sanidad catalana (VISC+).

En este contexto, hemos afrontado años con serias dificultades en la investigación con datos masivos. Por otra parte, no ha existido ninguna estrategia para la captación de donaciones de datos para la investigación en salud ¡en el país con mayor número de donantes de órganos! COVID-19 nos enfrenta a un proceso de investigación clínica acelerada y de transferencia inmediata de herramientas a los servicios de salud. El talento entero de una nación se ha puesto al servicio de la ciencia, la tecnología y la atención a los enfermos en un esfuerzo sin precedentes.

Siempre que es posible inicio y finalizo mis intervenciones afirmando que la grandeza del derecho a la protección de datos reside en que protegemos a las personas. Con los planteamientos de algunas autoridades de protección de datos y del Comité Europeo de Protección de Datos ¿a qué personas protegemos? ¿Es razonable que respondamos a estas cuestiones desde un positivismo jurídico hipergarantista?

En mi opinión ha llegado el tiempo del «cómo», y autoridades y expertos podemos y debemos contribuir en el esfuerzo. Este trabajo trata de acreditar que existen bases jurídicas razonables para todos los posibles tratamientos. Y también de desterrar temores infundados. Las autoridades sanitarias actúan con pleno sometimiento al Derecho y bajo el control de una autoridad independiente, cuando no de la justicia. Y necesitan a unos expertos en protección de datos que salgan de su confortable zona de campeones del no, y desplieguen una enorme

vocación de servicio, de dedicación a la comunidad como aliados en la guerra contra la enfermedad.

(1)

PUEYO Tomas. Coronavirus: Why You Must Act Now. Politicians, Community Leaders and Business Leaders: What Should You Do and When? Disponible en https://medium.com/@tomaspueyo/coronavirus-act-today-or-people-will-die-f4d3d9cd99ca. [consulta: 16 de marzo 2020]. Puede verse también una simulación en STEVENS, Harry. Why outbreaks like coronavirus spread exponentially, and how to «flatten the curve». En The Washington Post [en línea]. Disponible en https://www.washingtonpost.com/graphics/2020/world/corona-simulator/ [consulta: 16 de marzo 2020].
Ver Texto

(2)

NOTA DE PRENSA. Statement of the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak. Disponible en https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en [consulta: 16 de marzo 2020].
Ver Texto

(3)

ICO. Data protection and coronavirus. Disponible en https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/03/data-protection-and-coronavirus/ [consulta: 16 de marzo 2020].
Ver Texto

(4)

PADÍN Alejandro. COVID-19. Opiniones de las autoridades de supervisión europeas en materia de protección de datos personales. Disponible en https://www.padin.com/2020/03/listado-de-recursos-online-con-las.html [consulta: 16 de marzo 2020].