
FACULTAD DE DERECHO

# RASTREO TELEFÓNICO Y PROTECCIÓN DE DATOS: LÍMITES Y GARANTÍAS LEGALES

Autor: Agustín Díaz Vidriales
5º E3 A
Derecho Civil

Tutor: José María Ruiz de Huidobro de Carlos

## ÍNDICE

**LISTADO DE ABREVIATURAS**

ESPII: Emergencia de Salud Pública de Importancia Internacional

OMS: Organización Mundial de la Salud

GPMB: *Global Preparedness Monitoring Board*

RGPD: Reglamento General de Protección de Datos

LOPD: Ley Orgánica de Protección de Datos

L. Org.: Ley Orgánica

UE: Unión Europea

Arts.: artículos

AEPD: Agencia Española de Protección de Datos

ADN: Ácido desoxirribonucleico

ANM: Academia Nacional de Medicina

NHS: *England´s National Healthcare Service*

## INTRODUCCIÓN

La protección de datos personales es un tema cuya importancia está creciendo a un ritmo muy elevado en la actualidad. La trascendencia del mismo se ha visto incrementada exponencialmente durante el último año, principalmente como consecuencia de la pandemia ocasionada por el COVID-19.

El 31 de diciembre de 2019, la Comisión Municipal de Salud y Sanidad de Wuhan (provincia de Hubei, China) informa acerca de 27 casos de infección pulmonar de causa desconocida. Estas 27 personas tenían en común haber estado en un mercado de marisco, pescado y animales vivos en la ciudad de Wuhan.
El 8 de diciembre, el primer caso comenzó a presentar los primeros síntomas. Las autoridades chinas, el 7 de enero de 2020, comunicaron que la causa era un virus, hasta el momento, desconocido, perteneciente a una familia de virus llamada "Coronaviridae" (coronavirus).

El COVID-19 se expandió rápidamente por el mundo, y, durante la reunión que mantuvieron el 30 de enero de 2020, el Comité de Emergencias del Reglamento Sanitario Internacional (RSI, 2005) declaró el brote como una ESPII.
Posteriormente, el 11 de marzo, la OMS, declaró la pandemia mundial. Desde el inicio de la epidemia hasta el 11 de julio se han confirmado más de 12 millones de casos en todo el mundo, siendo aproximadamente 254.000 de ellos en nuestro país.

Esta pandemia ha provocado una gran crisis sanitaria como consecuencia del gran número de personas infectadas, el riesgo para la población general y la saturación del sistema sanitaria durante los meses del pico de la pandemia en nuestro país y en muchos otros países del mundo, donde la situación sigue siendo grave.

Aunque la comunidad internacional ha realizado grandes esfuerzos para diagnosticar y controlar mejor la enfermedad, como se ha visto reflejado en el desarrollo de una vacuna, es probable que la situación siga siendo crítica.

No es la primera vez que nos enfrentamos a una pandemia, aunque nunca se ha propagado a la velocidad de esta. Recientemente, situaciones como la gripe de 2009 y el ébola,

sirvieron como ejemplo para que organismos internacionales alertasen sobre el futuro. Los integrantes del GPMB, formado por expertos tanto de la OMS como del Banco Mundial, anunciaban en 2019 la poca preparación que teníamos a nivel mundial para prevenir las posibles futuras pandemias, que podían ocasionar millones de muertos y una gran repercusión sobre la economía global, retroceso que ya hemos empezado a sufrir.

Los sistemas de información sanitaria y de vigilancia epidemiológica generan gran cantidad de información compleja, que ha de ser analizada con estrategias de tratamiento masivo de datos. Dicho análisis permitirá valorar de mejor manera el impacto que el coronavirus está teniendo, tanto a nivel nacional como internacional. Además, esta información puede aportar grandes beneficios a la sociedad en su conjunto, permitiéndonos afrontar en mejores condiciones nuevas posibles oleadas de esta pandemia u otras posteriores.

Uno de los mecanismos para conseguir la realización de dicho análisis es el de una aplicación de rastreo telefónico. Es por ello que el objetivo de este trabajo consiste en, una vez analizado el entorno legal, tratar de determinar las garantías legales que dicha aplicación debería cumplir.

Para ello, analizaré en primer lugar las cuestiones técnicas relacionadas con dicho tratamiento. Aparecen aquí cuestiones como el concepto de big data o sus características, así como sus aspectos positivos y negativos y los retos a los que nos enfrentamos con la aplicación del mismo.

Posteriormente, me centraré en el ámbito de la protección de datos personales. Primero analizaré el entorno legal en el que se encuentra, estudiando tanto la normativa jurídica aplicable como las recomendaciones de las agencias europeas de protección de datos. A continuación, detallaré los principios aplicables al tratamiento de datos personales, estudiando aquí todos los principios que dicho tratamiento ha de respetar.

Por último, me enfocaré en la aplicación de rastreo. En este apartado, consideraré la recogida de datos por parte de otro tipo de aplicaciones, las partes del contrato del que entramos a formar parte cuando descargamos una aplicación, los principios aplicables al

caso concreto de una aplicación de rastreo y el uso secundario de nuestros datos que la misma pueda hacer.

Además, también he de hacer referencia al Diploma de Fundamentos de Legal Tech y Business Analytics que realicé en esta Universidad durante el curso pasado. Dicho diploma me sirvió tanto para adquirir conocimientos acerca del ámbito de la protección de datos como para conocer las recomendaciones que distintas agencias realizaban sobre la materia, gracias a la memoria que entregué al concluir el diploma. Así, con la realización de este trabajo he tenido la oportunidad de utilizar y ampliar los conocimientos adquiridos con la realización del mencionado diploma.

## CAPÍTULO I. CUESTIONES TÉCNICAS: EL BIG DATA

### 1. CONCEPTO DE BIG DATA

Como concepto, el big data es tremendamente abstracto, ya que no existe consenso sobre el mismo en la literatura.

Una de las definiciones que mejor recoge el concepto se encuentra en el informe "*Big data: the next frontier for innovation, competition and productivity*", de McKinsey Global Institute, que lo define como aquellas bases de datos que debido a su tamaño, complejidad y variedad de información que contienen no pueden ser almacenadas y gestionadas mediante *software* tradicional y necesitan el uso de herramientas específicas.[1]

### 2. LAS CINCO UVES

En muchas ocasiones, el big data se ve asociado con las "cinco uves del big data". Esas cinco uves hacen referencia a cinco características fundamentales del big data: volumen, variedad, velocidad, veracidad y valor. Dichas propiedades pueden aplicarse a cualquier sector en el que el big data sea de aplicación, por lo que pueden encontrarse desde el área empresarial hasta el ámbito de la medicina.[2]

En el primer caso, el análisis de un gran volumen de datos resulta muy útil para entender el perfil, las necesidades y el sentir que los consumidores respecto a los productos y/o servicios que la empresa ofrece en el mercado. También da la posibilidad a la empresa de analizar a sus competidores y mejorar la forma en la que interactúa en el mercado en sus relaciones con sus *stakeholders*.

Por su parte, el sector de la medicina genera enormes cantidades de datos diariamente, ya que los nuevos pacientes son continuamente sometidos a pruebas.

---

[1] Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., & Byers, A. H."Big data: The next frontier for innovation, competition, and Productivity". *McKinsey & Company*

[2] Ishwarappa, & Anuradha, J. "A brief introduction on Big Data 5Vs Characteristics and Hadoop Technology". *Procedia Computer Science 48*

## 2.1. Volumen

La primera de las uves a analizar es el volumen. Partiendo de la propia definición del concepto de big data elaborado por Mckinsey Global Institute [3], es necesario que la base de datos sea de tal tamaño que supere la capacidad del software tradicional para ser almacenados y gestionados.

Cabe decir también que los continuos avances tecnológicos que se producen hace que el concepto de volumen esté en continuo cambio. Esto se debe a que dichos avances provocan que sea posible el tratamiento de volúmenes de datos cada vez de mayor tamaño.

## 2.2. Variedad

La segunda uve es la variedad. Este aspecto hace referencia a que los datos no son siempre homogéneos y estructurados, ya que en ese caso sería posible su gestión con software tradicional. Así, se incluyen otros tipos de fuentes de datos diferentes a las que se utilizan de forma habitual.

Dicha variedad de datos, a su vez, se puede subdividir en cinco categorías. La subdivisión de la variedad de los datos realizada por Cottle [4] es de gran utilidad en el ámbito sanitario. De esta manera, es posible encontrar:

- Datos de la web y redes sociales: incluye datos de interacción tanto en redes sociales como en blogs. Además, puede incluir otros aspectos como aplicaciones para teléfonos inteligentes o sitios web de planes de salud.
- Datos de máquina a máquina: incluye principalmente medidores y sensores.
- *Big transaction data*: consiste en una transacción de información dentro de un sistema informático de elementos tecnológicos. Principalmente incluye registros de facturación y reclamaciones de atención médica.

[3] Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., & Byers, A. H."Big data: The next frontier for innovation, competition, and Productivity". *McKinsey & Company*

[4] Cottle, M., Kanwal, S., Kohn, M., Strome, T., & Treister, N. "Transforming health care through Big Data". *Institute for health technology transformation*

- Datos biométricos: huellas dactilares, escritura a máquina, presión arterial, datos recogidos mediante tecnologías de reconocimiento facial…
- Datos generados por los humanos: en el ámbito de la medicina incluye correos electrónicos, documentos en papel, así como otro tipo de información generada por el personal sanitario.

### 2.3. Velocidad

La tercera uve está asociada con el elevado ritmo al que se produce, gestiona y transmite la información. Así, este concepto se refiere a la rapidez con que los datos se reciben y procesan para tomar decisiones a partir de ellos, ya que a la gran mayoría de sistemas de software tradicional les es imposible analizar de manera inmediata la información que reciben.

En el caso concreto del ámbito sanitario existen numerosos ejemplos donde esta característica se ve reflejada. Uno de ellos sería el sujeto al que se le instala un aparato electrónico que informa a un laboratorio constantemente de sus constantes vitales, permitiendo a los trabajadores del laboratorio la realización de un estudio de su situación en tiempo real.

De esta forma, esta característica supone un desafío de enorme magnitud para los , al tener continuamente que adaptarse a nueva información que reciben constantemente, de tal forma que siempre hay algún dato nuevo que afecta al resultado de la investigación. También supone una oportunidad, ya que es posible recibir información en el momento en que se produce y tener la capacidad de manejarla.

### 2.4. Veracidad

La cuarta uve hace referencia a la realidad de que no toda la información de la que está compuesta una base de datos de big data es veraz. Nos referimos a la veracidad para explicar la calidad y fiabilidad de los datos, así como el grado de confianza que el procesador tiene en los mismos a la hora de tratarlos.

El resto de características que conforman el concepto de big data dan lugar a la posibilidad de combinar diversas fuentes de datos. Consecuentemente, la información sea más fiable y el resultado será más certero, por lo que será posible una mejor toma de decisiones.

### 2.5. Valor

La definición del valor del dato por sí misma es fundamental, ya que hace referencia a la información útil que vamos a poder extraer de los datos. Esta información fomentará la generación de un valor que podrá ser convertido en conocimiento y, consecuentemente, utilizado para la toma de decisiones. Consecuentemente, el valor es probablemente el aspecto más importante en el ámbito del big data.

En el ámbito sanitario, destaca el estudio realizado por la revista Health Affair [5], según el cual la aplicación del big data al mundo de la medicina puede generar una enorme reducción de costes. Dicha aplicación, unida a otros beneficios que traería consigo, podría resultar en la generación de un valor adicional para los servicios sanitarios de 300 mil millones de dólares al año.

## 3. ASPECTOS POSITIVOS

El aspecto positivo más importante del big data es el elevado número de oportunidades que su aplicación ofrece. La realidad es que se encuentra en constante evolución y cambio, por lo que muchas de las posibilidades que permite su aplicación aún no han sido descubiertas.

En el ámbito de la salud pública, el análisis masivo de datos mediante la aplicación de big data permite gestionar una cantidad muy elevada de información. Esta información convertida en datos de los pacientes constituye una información de tremendo valor. Por un lado, desde el punto de vista del paciente, facilitaría su seguimiento y evolución. Por otro lado, respecto del punto de vista de la gestión sanitaria, evitaría duplicidades innecesarias y optimizaría los recursos de los que dispone. Además, gracias a la característica de la velocidad, sería posible la detección precoz de epidemias.

[5] Roski J, Bo-Linn GW, Andrews TA. Creating value in health care through big data: opportunities and policy implications. *Health Affair*

PLANAS [6] indica que cada siglo se producen dos revoluciones en el sector sanitario basadas en las tendencias de la época. En la actualidad, esa tendencia sería el elevado volumen de datos que existen. En este sentido, el mismo autor señala que las herramientas y la sistematización de la atención al paciente tendrán efecto tanto en la forma de trabajar de los médicos como en el trato que los pacientes reciben en los hospitales.

RODRIGO LARRUCEA [7] defiende que, gracias a que el correcto uso del big data asegura la privacidad de las personas, nos encontramos ante un abanico enorme de oportunidades para el estudio de estadísticas y datos biométricos. Dicha información podrá ser tenida en cuenta para el diseño de estrategias sanitarias a medio y largo plazo, provocando una mejora de las mismas.

En la jornada "Hacia un sistema sanitario basado en la creación de valor: La era de los datos, nuevo paradigma en la financiación de fármacos innovadores" [8], especialistas de distintas regiones y diferentes ámbitos del amplio sector sanitario analizaron las expectativas que se presentan ante el desarrollo de técnicas de big data y su aplicación en el campo de la medicina. Durante la misma, llegaron a la conclusión de que el big data supondrá un cambio de paradigma tanto para extraer conclusiones como para tomar decisiones.

Consecuentemente, otro de los importantes avances que presenta la aplicación de técnicas de big data en el ámbito de la salud es que tiene la capacidad, gracias al análisis y almacenamiento de diversas fuentes de información, de responder preguntas sin necesidad de realizar una investigación puntual.
Este era un paso que en un primer momento se preveía complicado. Sin embargo, gracias al desarrollo continuo de nuevas tecnologías, a día de hoy es viable.

Otro aspecto a destacar es los beneficios que tiene para las personas cuyos recursos económicos son escasos. Un gran número de personas ven imposible el acceso a muchos

---

[6] Planas, J. "BIG DATA Revolución en el sector sanitario - Dr. Jorge Planas*". Dr. Jorge Planas Blog Personal*

[7] Rodrigo Larrucea, C. "Mhealth y Bigdata en sanidad". *Derecho y Salud no van siempre de la mano.*

[8] Fundación Instituto Roche – "III Jornada «Hacia un Sistema Sanitario basado en la creación de Valor". *El médico interactivo*

servicios médicos, al no contar con los recursos necesarios para ello. Sin embargo, el big data contribuye a democratizar el acceso a la medicina, gracias a la digitalización y mayor difusión del conocimiento médico.

Un último aspecto positivo que el big data puede tener en el mundo de la sanidad es relativo al ámbito de la genética. La gran cantidad de muestras de las que disponen los investigadores provoca que la secuenciación de ADN sea una tarea paulatinamente más asequible. Consecuentemente, los avances que se produzcan en esta área irán de la mano de la posibilidad de analizar los datos de manera masiva. Así, la aplicación de técnicas de big data resulta el instrumento más adecuado para la realización de esa labor. [9]

## 4. ASPECTOS NEGATIVOS

Pese a que está claro que el big data tiene efectos positivos en el ámbito sanitario, su implementación no está exenta de preocupaciones. Dichas preocupaciones provienen principalmente del sector jurídico.

Desde el punto de vista de PARRA CALDERÓN [10], a medida que aumenta la aplicación de técnicas de big data se identifican nuevos retos a los que enfrentarse en su implementación. Consecuentemente, la aplicación de técnicas de big data nunca estará exenta de riesgos.

Por otro lado, LLÁCER, CASADO y BUISAN [11] indican que existe la posibilidad de que los datos de pacientes sean proporcionados a empresas que pueden utilizarlos, ya sea para comercializar con ellos o en su propio beneficio. Esta realidad, según indican, dista mucho de la utilización de los datos de pacientes con fines de investigación.

---

[9] O'Driscoll, A., Daugelaite, J., & Sleator, R. D. (2013). "'Big data', Hadoop and cloud computing in genomics". *Journal of Biomedical Informatics*

[10] Calderón, P. C. L. "Big data en sanidad en España: la oportunidad de una estrategia nacional". *Parra Calderón*

[11] Llácer Matacás, MªR., Casado, M., BUISAN ESPELETA, L. *Documento sobre bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública*

Para GIL GONZÁLEZ [12], existe el riesgo de caer en conclusiones erróneas que nadie analice. Dicho de otra manera, la posibilidad de que las personas tomen decisiones automatizadas sin revisar previamente la información en la que se basan para ello.

Otra de las preocupaciones que existen acerca del uso de big data se encuentra en las dificultades técnicas del almacenamiento de una magnitud de datos tan grande. Esta preocupación está íntimamente relacionada con aquella relativa a la seguridad de dicho almacenamiento, haciendo inviable su robo o *hackeo*.

La preocupación más importante, que incluye a muchas de las anteriores, es relativa al derecho a la intimidad. Los principales problemas en este sentido se refieran a la vulneración de la privacidad, así como a la falta de consentimiento en el uso de los datos.

La preocupación relativa a la vulneración de la privacidad se vio reflejada en las tesis de Llácer, Casado y Buisan. El principal resultado de esta situación sería que tanto el controlador como el procesador de los datos de una persona supieran más acerca de la persona que el propio interesado.

La preocupación relativa al consentimiento informado se refiere a la ausencia de autorización con conocimiento por parte del interesado. En esta situación, sus datos clínicos serían tratados en una investigación científica sin que el paciente fuera conocedor de dicha investigación.

A este respecto, es importante destacar el denominado sesgo del consentimiento. Este problema, según la ANM, se da en situaciones en las que *"los sujetos que dan permiso para que se acceda a su información médica difieren del grupo de individuos que se muestran contrarios a dar permiso para que su información médica se use en investigación"* [13]. Esta realidad provoca que el conjunto de pacientes dispuestos a ceder su información médica para una investigación científica no tienen las mismas características que aquellos que se oponen. Un ejemplo de esta situación es aquella investigación en la que los jóvenes están de acuerdo en la cesión de su información y las

[12] Gil González, E. *Big Data, privacidad y protección de datos.*
[13] Nass, S. J., Levit, L. A., & Gostin, L. O. (Eds.). (2009). "Beyond the HIPAA Privacy Rule". *Institute of Medicine*

personas de edad más avanzada se oponen a la misma. El principal resultado es la imposibilidad de llegar a conclusiones válidas para todos los pacientes, por lo que han de ser adaptadas al grupo que no se opuso a la cesión de sus datos.

## 5. RETOS

Los dos principales retos que presenta la implementación de técnicas de big data en el ámbito sanitario se refieren a la recopilación y gestión de los datos, así como a la protección de la intimidad y privacidad frente al avance tecnológico.

### 5.1. Recopilación y gestión de los datos

La propia definición de big data hace referencia a un gran conjunto de datos e información, cuyo elevado tamaño hace imposible su almacenamiento y análisis con herramientas de gestión de bases de datos tradicionales. La cuestión es relativa al acceso, distribución y utilización de los datos no estructurados.

Según el informe de Siemens "*Healthcare Dives into Big Data*", [14] más del 80% de los datos de salud no se encuentran estructurados y se almacenan de forma diferente según sus características (transcripciones médicas, pruebas de laboratorio…).

Los retos que caracterizan la aplicación de big data en el ámbito de la medicina son la gran variedad en la naturaleza de los datos y la alta velocidad de proceso que se requiere. El problema consiste en que la información necesaria para evaluar correctamente la situación del paciente y el tratamiento que más le conviene está disponible en un formato de datos no estructurados, que habitualmente es las anotaciones del médico. De esta manera, sin los instrumentos necesarios ese conocimiento seguiría sin estar disponible, y no sería posible utilizarlo. Así, es necesario encontrar un sistema para poder monitorizar y procesar esa información, para que pueda ser aprovechada en beneficio de la salud del paciente.

[14] Siemens. "*Healthcare Dives into Big Data"*.

También es destacable en este sentido el informe emitido por la Casa Blanca durante la administración de Barack Obama, [15] quien se comprometía a destinar 200 millones de dólares a investigación y desarrollo en el ámbito del big data. Dicho informe detallaba que el dinero serviría para mejorar las técnicas y herramientas de acceso y organización de grandes volúmenes de datos digitales. A su vez, destacaba la utilización del big data como un mecanismo de progreso en el descubrimiento científico, la educación, el medio ambiente, la seguridad nacional y la investigación biomédica.
Dicho informe también destaca los avances y ventajas que la implementación de técnicas de big data tendrá sobre otros datos relacionados con la salud y la enfermedad, como la imagen molecular y el conocimiento celular.

### 5.2. Protección de la intimidad y privacidad frente al avance tecnológico

El otro gran reto al que se enfrenta el big data consiste en combinar el derecho a la privacidad e intimidad de la persona con los avances tecnológicos requeridos para la implantación del big data.

Respecto a este punto, Tim Kelsey, [16] cuando era director del NHS, defendía que el sistema de salud ha de salvar vidas y este fin ha de prevalecer sobre cualquier otro. El ejemplo del Reino Unido fue seguido por otras regiones, como prueba el proyecto VISC+ de Cataluña.

Pese a que esa perspectiva tuvo una fuerte oposición por parte de grupos garantistas de la privacidad de la información, lo cierto es que todos los proyectos se han comprometido a cumplir los protocolos de anonimización de datos, aplicando la normativa de la manera más estricta posible para dar las máximas garantías de seguridad.

[15] "Obama Administration Unveils "BIG DATA" Initiative: Announces $200 Million in New R&D Investments", *IEEE Signal Processing Society*
[16] Curtis, J. "NHS boss claims patient data collection is «morally right»". *IT PRO*

## CAPÍTULO II. PROTECCIÓN DE DATOS PERSONALES

### 1. ANÁLISIS DEL ENTORNO LEGAL

A la hora de analizar la posibilidad de crear una aplicación que informase acerca de la situación médica de las personas, es importante tener en cuenta el entorno legal sobre el cual dicha aplicación se desarrollaría. Es por ello necesario analizar la normativa jurídica existente en la materia de la protección de datos, así como las recomendaciones que distintas agencias de protección de datos realizan acerca de su interpretación.

Para el análisis de la normativa jurídica aplicable, me he centrado en el Reglamento General de Protección de Datos, así como en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

El Reglamento General de Protección de datos establece un régimen de protección de datos en la Unión Europea, ampliando su alcance a empresas extranjeras que tratan datos de ciudadanos residentes en la Unión Europea, ofreciendo un nuevo conjunto de derechos digitales para sus ciudadanos.

El Título X de la Ley Orgánica 3/2018 acomete la tarea de reconocer y garantizar un elenco de derechos digitales de los ciudadanos conforme al mandato establecido en la Constitución, regulando particularmente los derechos y libertades predicables al entorno de Internet. De esta forma, aspectos como la neutralidad de la Red, el acceso universal a la misma, los derechos al olvido o a la seguridad y la educación son algunas de las novedades que dicha ley introduce en nuestro ordenamiento jurídico. Ocupa un lugar relevante el reconocimiento del derecho a la desconexión digital en el marco del derecho a la intimidad en el uso de dispositivos digitales en el ámbito laboral y la protección de los menores en internet. Finalmente, resulta destacable la garantía de la libertad de expresión y el derecho a la aclaración de informaciones en medios de comunicación digitales. En resumen, tiene el propósito de actualizar la obsoleta Ley Orgánica de Protección de Datos de Carácter Personal, aprobada en 1999, al incluir el ámbito relativo a los derechos digitales.

Por otra parte, también he consultado las páginas web de las distintas agencias de protección de datos e instituciones relacionadas con ella, realizando una búsqueda con el texto "Covid-19".

- Agencia Española de Protección de Datos
- *European Data Protection Board*
- Eur-Lex. El acceso al Derecho de la Unión Europea
- *Council of Europe Data Protection website*
- Otras instituciones
    - *The Global Privacy Assembly (GPA) and The Organisation for Economic Co-operation and Development (OECD)*
    - Otras instituciones oficiales en protección de datos durante la pandemia de COVID-19

## 1.1. Análisis de la normativa jurídica

### *1.1.1. Reglamento General de Protección de Datos* [17]

Los aspectos más importantes a tener en cuenta a la hora de analizar el Reglamento General de Protección de Datos son: su ámbito de aplicación, la base legal para el tratamiento, el consentimiento y la seudonimización.

En primer lugar, respecto al ámbito de aplicación, la regulación será aplicable para aquellos casos en los que la organización que recolecta los datos (controlador), la organización que simplemente trata los datos en nombre del controlador de datos (procesador) o las personas cuyos datos son recolectados (interesado) son residentes en la UE, así como para aquellos supuestos en los que organizaciones cuya sede no se encuentre dentro de la UE recopilen datos personales de residentes de la UE. De acuerdo con la definición dada por parte de la Comisión Europea, los datos personales se refieren a cualquier información relacionada con un individuo, independientemente de que se refiera a su vida privada, profesional o pública.

[17] Reglamento General de Protección de Datos 2016/679

En segundo lugar, queda establecida la necesidad de que exista una base legal que justifique el tratamiento de datos. Así, es necesario que se de al menos una de las siguientes condiciones:

- El interesado ha dado su consentimiento, siendo conocedor de los propósitos específicos.
- El tratamiento es necesario para la ejecución de un contrato por parte del interesado.
- El tratamiento es necesario para que el controlador cumpla una obligación legal a la que está sujeto.
- El tratamiento es necesario para la protección de los intereses vitales de alguna persona física.
- El tratamiento es necesario por razones de interés público.
- El tratamiento es necesario para los fines de los intereses legítimos perseguidos por el responsable o por un tercero.

En tercer lugar, en lo que al consentimiento se refiere, los arts. 4 y 7 del RGPD establece que cuando el consentimiento se utiliza como base legal para el tratamiento, ha de ser explícito para los datos recopilados y los objetivos que se pretenden conseguir con la recopilación.

Por último, en cuanto a la seudonimización, cabe decir que los arts. 33 y 34 del RGPD señalan que, en los supuestos en los que la información está cifrada, la producción de una fuga no implica la necesidad de notificar ni a los afectados ni a la autoridad administrativa correspondiente en cada región. De esta forma, la encriptación de los datos es considerada por el RGPD como el mecanismo más seguro para lograr su protección.

### *1.1.2. Mención especial a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales* [18]

La L.Org. 3/2018, de 5 de diciembre, tiene por objeto la adaptación del ordenamiento jurídico español en materia de protección de datos al RGPD. De esta forma, deroga la

[18] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal [19], y añade a nuestro marco normativo el ámbito relativo a los derechos digitales.

## 1.2. Análisis de las recomendaciones de las agencias europeas de protección de datos

### 1.2.1. *Agencia Española de Protección de Datos* [20]

En primer lugar, respecto a la Agencia Española de Protección de Datos, nos podemos encontrar con el Informe sobre el tratamiento de datos personales en relación con la situación derivada de la extensión del virus COVID-19, [21] así como con El uso de las tecnologías en la lucha contra el COVID-19, un análisis de costes y beneficios [22].

El "Informe sobre el tratamiento de datos personales en relación con la situación derivada de la extensión del virus COVID-19" no hace referencia específica al análisis masivo de datos, sino simplemente se remite al RGPD, que permite el tratamiento de datos personales de salud sin consentimiento del interesado no solo en el ámbito de la salud pública sino también en el cumplimiento de las obligaciones legales en el ámbito laboral derivado de las mismas.

Los responsables de esos tratamientos, al estar actuando para salvaguardar dichos intereses, deberán actuar conforme a lo que las autoridades establezcan en la normativa del Estado correspondiente (en este caso, España).

En "El uso de las tecnologías en la lucha contra el COVID-19. Un análisis de costes y beneficios", la AEPD publica un estudio en el que analiza distintas tecnologías para luchar contra el coronavirus, y los riesgos que cada una de ellas tiene para la privacidad. Así, la Agencia examina en el documento la relación entre los posibles beneficios para el control de la pandemia y los riesgos para la privacidad que implica la utilización de estas tecnologías.

---

[19] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
[20] Agencia Española de Protección de Datos. Página web oficial
[21] Agencia Española de Protección de Datos. "Informe sobre el tratamiento de datos personales en relación con la situación derivada de la extensión del virus COVID-19".
[22] Agencia Española de Protección de Datos. "El uso de las tecnologías en la lucha contra el COVID-19. Un análisis de costes y beneficios".

En este sentido, el informe realiza un análisis preliminar de siete sistemas: geolocalización recogida por los operadores de telecomunicaciones; geolocalización en redes sociales; apps, webs y chatbots para auto-test o cita previa; apps de información voluntaria de contagios; apps de seguimiento de contactos por Bluetooth; pasaportes de inmunidad y cámaras infrarrojas.

Como se indica, en este documento se realiza un breve repaso de las principales tecnologías planteadas en la lucha contra la pandemia, sin pretender realizar un análisis profundo de las mismas, con el propósito de compilar aquellas opciones que se están manejando para controlar su expansión.

Nuestra sociedad se encuentra en un punto crítico de inflexión, tanto como consecuencia de la pandemia como en cuanto al planteamiento del modelo existente de derechos y libertades. De esta manera, resulta vital ser extremadamente cuidadoso a la hora de tomar medidas, ya que estas pueden tener consecuencias irreversibles. Otro motivo es que estas medidas pueden estar guiadas únicamente por la urgencia, el miedo o, lo que es peor, otros intereses.

En este aspecto, resulta necesario recordar que las tecnologías de la información no han de ser entendidas de forma aislada, sino siempre en el marco de un tratamiento con una finalidad determinada. Dicho tratamiento ha de implementar una estrategia global partiendo de la base de evidencias científicas, evaluando su proporcionalidad en cuanto a su eficacia y eficiencia. Asimismo, habrá que tener en cuenta los recursos organizativos y los materiales necesarios. De igual manera, habrá que prestar atención al cumplimiento de los principios recogidos en el RGPD.

Dentro de lo relativo a la Agencia Española de Protección de Datos, si bien no son documentos como tal, resulta también necesario hacer referencia a dos ciclos de conferencias. Por un lado, “Innovación, protección de datos y salud (I). Soluciones tecnológicas para combatir la COVID-19”. Por otro lado, “Innovación, protección de datos y salud (II). Bioética y Derecho. Proteger la privacidad en la sociedad digital post COVID-19”.

El primero de ellos fue un seminario a cargo de Carmela Troncoso, enfocado a la construcción de sistemas y el desarrollo de metodologías que contribuyan a reforzar las garantías de privacidad en sus diseños y la búsqueda de soluciones que posibiliten el

intercambio seguro de datos genéticos. Carmela Troncoso, además, está liderando la creación de una app a nivel europeo para rastrear contagios de COVID-19. [23]

El segundo de ellos fue un seminario a cargo de Itziar de Lecuona, con el que la Agencia Española de Protección de Datos pretende promover un debate sobre las consecuencias que ha podido traer el COVID-19 para la privacidad. En otras palabras, promueve la reflexión acerca de cómo proteger mejor el derecho fundamental a la protección de datos en la "nueva realidad". [24]

### *1.2.2. European Data Protection Board* [25]

En cuanto a los documentos de esta Agencia, destaca, en primer lugar, "*Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak*" (cuya traducción se asimilaría a "Recomendaciones en el procesamiento de datos en el ámbito sanitario con el propósito del desarrollo científico en el contexto de la expansión del coronavirus"). [26]

Si bien este documento no hace ninguna referencia específica al tratamiento masivo de datos, al remitirse únicamente al RGPD y a las leyes de cada Estado, este documento tiene la finalidad de intentar clarificar las cuestiones legales más urgentes en relación al tratamiento de datos de salud, como las bases legales para su procesamiento, la implementación de medidas adecuadas de protección y el ejercicio que cada sujeto pueda hacer de sus derechos en relación al tratamiento de sus datos.

Este documento contiene varias provisiones para el procesamiento de datos de salud con el propósito del desarrollo científico, por lo que también resulta aplicable en el contexto de la pandemia provocada por el COVID-19, particularmente en lo concerniente al consentimiento y a las respectivas legislaciones nacionales.

---

[23] Agencia Española de Protección de Datos. Webinario "Innovación, protección de datos y salud (I). Soluciones tecnológicas para combatir el COVID-19".
[24] Agencia Española de Protección de Datos. Webinario 'Innovación, protección de datos y salud (II)'. Bioética y Derecho. Proteger la privacidad en la sociedad digital post COVID-19.
[25] European Data Protection Board. Página web oficial
[26] European Data Protection Board. Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak

En nuestro caso, el propio Reglamento General de Protección de Datos prevé la posibilidad del procesamiento de ciertas categorías especiales de datos personales, entre los que se encuentran los datos relacionados con la salud, cuando sea necesario para fines científicos.

Además, las recomendaciones solucionan cuestiones legales relativas a la transferencia internacional de datos, entre los que se incluyen aquellos relacionados con la salud, con propósitos de investigación en la lucha contra el COVID-19, particularmente en casos en los que se produzca la falta de decisiones de adecuación apropiadas.

Andrea Jelinek, directiva del *European Data Protection Board* (Comité Europeo de Protección de Datos), indica "actualmente, se están realizando grandes esfuerzos de investigación en la lucha contra el coronavirus. Los investigadores tienen la esperanza de obtener resultados tan pronto como sea posible. El Reglamento General de Protección de Datos no impide la investigación científica, sino que permite el procesamiento legítimo de datos de salud para tener más posibilidades de encontrar una vacuna o un tratamiento para el COVID-19". (resumen original en el Anexo)

En segundo lugar, el documento "*Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*" (cuya traducción sería "recomendaciones en el uso de datos de localización y herramientas para el rastreo de contactos en el contexto de la propagación del COVID-19") sí hace referencia al tratamiento masivo de datos, haciendo especial hincapié en la anonimización de los mismos. [27]

Este documento intenta clarificar las condiciones y principios aplicados al uso proporcionado y apropiado de las herramientas para el rastreo de contactos y de los datos de localización para dos propósitos principales:

1. Las herramientas para el rastreo de contactos tiene la finalidad de informar a aquellos individuos que han estado próximos a alguien que termina siendo

[27] European Data Protection Board. Guidelines 04/2020 on the use of location data and contract tracing tools in the context of the COVID-19 outbreak

confirmado como un portador del virus, con la finalidad de romper las cadenas de contagio lo más rápido posible.

2. La utilización de datos de localización tiene la finalidad de facilitar la respuesta a la pandemia a través del modelamiento de la propagación del coronavirus para poder determinar la efectividad general de las medidas implementadas.

Estas recomendaciones enfatizan que tanto el Reglamento General de Protección de Datos como la Directiva sobre *ePrivacy* contienen provisiones específicas que permiten el uso de datos anonimizados o personales para apoyar tanto a autoridades públicas como a otros actores, tanto a nivel nacional como a nivel de la Unión Europea, en sus esfuerzos para monitorizar y contener la propagación del coronavirus. Los principios generales de efectividad, necesidad y proporcionalidad deben servir como guía y referencia para cualquier medida adoptada por los Estados Miembros o las Instituciones de la Unión Europea que impliquen el procesamiento de datos personales en la lucha contra el COVID-19.

El Comité Europeo de Protección de Datos reitera la postura expresada en su letra a la Comisión Europea, de 14 de abril, en la que indicaba que el consentimiento para el uso de datos por parte de aplicaciones para el rastreo de contactos ha de ser voluntario y no basarse en movimientos individuales, sino en informar acerca de la proximidad con otros usuarios.

Andrea Jelinek añade que estas aplicaciones nunca pueden reemplazar a enfermeras ni a doctores. Mientras que los datos y la tecnología pueden ser herramientas tremendamente importantes, es necesario tener presente que tienen limitaciones intrínsecas. Las aplicaciones solamente pueden complementar la efectividad de las medidas públicas de seguridad y la dedicación de los trabajadores del campo sanitario acerca de la necesidad de la lucha contra el coronavirus. En ningún caso podrá la gente verse obligada a elegir entre una respuesta eficiente a la crisis y la protección de sus derechos fundamentales.

Además, el Comité Europeo de Protección de Datos ha adoptado una guía para las aplicaciones de rastreo de contactos con el propósito, si bien no es exhaustivo, de dar recomendaciones generales a los diseñadores e implementadores de aplicaciones de

rastreo de contactos, destacando que todas las evaluaciones que se quieran realizar han de ser llevada a cabo para cada caso concreto. (resumen original en el Anexo)

Ambos grupos de recomendaciones, como medida excepcional dada su urgencia, no serán sometidas a consulta pública, debido a la situación actual y a la necesidad de tener las recomendaciones disponibles cuanto antes.

### *1.2.3. Eur-Lex. El acceso al Derecho de la Unión Europea*

En cuanto a las instituciones reguladoras del Derecho de la Unión Europea, destacan la Recomendación 2020/518 de la Comisión [28] y la Comunicación que la Comisión realizó el 17 de abril de 2020 sobre aplicaciones móviles [29].

La Recomendación 2020/518 de la Comisión de 8 de abril de 2020 hace referencia a un conjunto de instrumentos comunes con los que cuenta la Unión para la utilización de la tecnología y los datos a fin de combatir y superar la crisis del COVID-19. Concretamente, se centra en lo referente a las aplicaciones móviles y a la utilización de datos de movilidad anonimizados.

Aquí, se recomienda que se realice un plan común paneuropeo para el uso de datos anonimizados y agregados sobre la movilidad de la población a fin de modelizar y predecir la evolución de la enfermedad, resaltando que los principios de protección de la intimidad y de los datos han de guiar la elaboración del conjunto de instrumentos.

Como indicaba anteriormente, también merece la pena destacar en este sentido la Comunicación de la Comisión acerca de las orientaciones sobre las aplicaciones móviles de apoyo a la lucha contra la pandemia de COVID-19 en lo referente a la protección de datos.

En este sentido, la propia comunicación destaca que las tecnologías y los datos digitales tienen una valiosa función que desempeñar en la lucha contra la crisis causada por la aparición del COVID-19. Las aplicaciones para dispositivos móviles que suelen estar

[28] Comisión Europea. Recomendación 2020/518
[29] Comisión Europea. Comunicación 124/I/01

instaladas en teléfonos inteligentes ("aplicaciones") pueden facilitar a las autoridades sanitarias públicas, tanto a nivel nacional como a nivel de la Unión Europea, el seguimiento y contención de la pandemia de COVID-19, y son especialmente pertinentes de cara al levantamiento de las medidas de confinamiento.

La injerencia en la intimidad y el derecho a la protección de los datos personales pueden ser aspectos especialmente significativos, dado que algunas de las funcionalidades se basan en un modelo de uso intensivo de datos.

Para garantizar el cumplimiento de la legislación de la UE en materia de protección de datos personales y de la intimidad, es necesario tener en cuenta los siguientes aspectos:

- Autoridades sanitarias nacionales (o entidades que realizan una misión que se lleva a cabo en favor del interés público en el ámbito de la salud) como responsables del tratamiento de datos
- Garantizar que la persona siga teniendo el control
- Base jurídica para el tratamiento
- Minimización de datos
- Limitar el acceso a los datos y su divulgación
- Tratamiento de los datos con fines precisos
- Establecimiento de límites estrictos al almacenamiento de datos
- Garantizar la seguridad de los datos
- Garantizar la exactitud de los datos
- Involucrar a las autoridades de protección de datos

### *1.2.4. Consejo de Europa* [30]

En cuanto a lo referente al Consejo de Europa, cabe destacar la Declaración Conjunta acerca del derecho a la protección de datos en el contexto de la pandemia del COVID-19 (en inglés, "*Joint Statement on the right to data protection in the context of the COVID-19 pandemic*"), dirigida por Alessandra Pierucci, Directiva del Comité de la Convención

[30] Consejo de Europa en materia de Protección de Datos en el ámbito del COVID-19. Página web

108 y Jean-Phillippe Walter, Comisario de Protección de Datos del Consejo de Europa, en Estrasburgo el 30 de marzo de 2020. [31]

En este sentido, dicha declaración indica que resulta crucial aclarar que la protección de datos no puede ser en ningún caso obstáculo para salvar vidas humanas. Además, hace referencia a que también es igualmente importante reafirmar que el ejercicio de los derechos humanos, especialmente los derechos de privacidad y protección de datos, no dejan en ningún momento de ser aplicables.

Los principios a seguir en materia de protección de datos siempre permiten ponderar los intereses tanto del fin que se quiere conseguir como del dato que se quiere proteger. La Convención 108 establece altos estándares para la protección de datos personales, haciéndola compatible y reconciliable con otros derechos fundamentales e intereses públicos relevantes.

Los principios consagrados en diversos instrumentos, tanto de carácter nacional como internacional, no pueden ser suspendidos. Únicamente podrían ser restringidos de manera legal, y por un tiempo determinado.

Ya que el tratamiento masivo de datos y las bases de datos están siendo generadas, al analizar los beneficios de las distintas técnicas de procesamiento de datos, como el Big Data o la Inteligencia Artificial, hay que tener en cuenta que ese conjunto de datos ha de ser procesado de tal manera que se garantice el respeto a la dignidad humana y a la protección de datos. Las recomendaciones realizadas por el Comité de la Convención 108 en el contexto del Big Data y la Inteligencia Artificial pueden resultar ser herramientas útiles tanto para los desarrolladores como para los gobiernos para modelar el procesamiento en una forma que garantice la protección contra el mal uso voluntario de datos y las consecuencias negativas inintencionadas que puedan darse, incluyendo entre ellas la discriminación a individuos o colectivos.

[31] Consejo de Europa. "Joint Statement on the right to data protection in the context of the COVID-19 pandemic"

La transparencia y la explicabilidad del análisis de datos o las soluciones de Inteligencia Artificial, las precauciones que se tomen y una estrategia de ponderación de los riesgos que se tomen (incluyendo el riesgo de reidentificación en los supuestos de datos anonimizados), el énfasis en la calidad de los datos y la minimización o el rol de los humanos que supervisen su tratamiento no son más que algunos de los apartados más importantes a tener en cuenta en el desarrollo de soluciones innovadoras en la lucha contra el COVID-19 (resumen original en el Anexo).

Así, los datos procesados para detectar y rastrear contactos deben ser reducidos al mínimo posible, provocando que todos los datos que no estén relacionados o sean estrictamente necesarios no deberán ser recogidos.

Los sistemas de detección de contactos han de estar sujetos a una vigilancia efectiva e independiente, así como a controles, para garantizar el respeto a los derechos de privacidad y la protección de datos.

Las autoridades relacionadas con la protección de datos han de estar involucradas desde el exterior en el desarrollo de tales sistemas, y tendrán que utilizar toda su capacidad de intervención e investigación para asegurar que el cumplimiento de los requisitos relacionados con los derechos de privacidad y protección de datos.

### *1.2.5. Mención especial a la GPA y la OECD*

a. La Asamblea de Privacidad Global (GPA, por sus siglas en inglés "Global Privacy Assembly") y la Organización para la Cooperación Económica Internacional y el Desarrollo (OECD, por sus siglas en inglés "Organisation for Economic Co-operation and Develpoment")

Dentro de las recomendaciones dictadas por estas organizaciones, destacan "Seguimiento y rastreo de la COVID: protegiendo la privacidad y los datos en el uso de aplicaciones y biometría" (en inglés, "Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics"), dictada el 14 de abril de 2020) [32]; y "Asegurando la

[32] The Global Privacy Assembly and The Organization for Economic Co-Operation and Development. "Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics".

privacidad de datos mientras luchamos contra el COVID-19" (en inglés "Ensuring data privacy as we battle COVID-19), dictada en la misma fecha. [33]

En cuanto a la primera, hace referencia a que las tecnologías digitales, particularmente las aplicaciones móviles y biométricas, están siendo adoptadas como innovaciones para mejorar la efectividad de las respuestas de los gobiernos frente al COVID-19.

Tanto la información resultante como las tendencias que analizan son extremadamente valiosas para que los gobiernos puedan seguir la evolución de la pandemia del COVID-19. Además, les permite alertar a comunidades y grupos especialmente vulnerables, así como comprender el impacto y la evolución que tienen el establecimiento de medidas tales como el confinamiento o el distanciamiento social.

El acceso a información personal puede permitir a la gente la mejor identificación de potenciales infecciones de COVID-19 y tener constancia de su propagación a lo largo del tiempo. Sin embargo, dentro de las soluciones que podrían darse a este respecto, no todas son totalmente respetuosas con los derechos a la privacidad y la protección de datos, por lo que no podrán aplicarse.

Así, las soluciones que se den no pueden interferir con una total transparencia y el mantenimiento y respeto de privacidad de las personas. Será necesario ponderar los beneficios y los riesgos asociados con la colección de datos personales, así como con su procesamiento y divulgación. De igual manera, estos datos deberán ser mantenidos únicamente el tiempo que sea estrictamente necesario para cumplir el objetivo que se pretendió cumplir al momento de recogerlos.

En cuanto a la segunda, hace referencia a que un gran número de gobiernos están llevando a cabo medidas sin precedentes para seguir, rastrear y contener el nivel de propagación del nuevo coronavirus. La principal medida a la que se refiere consiste en la utilización de tecnologías digitales y técnicas de análisis masivo para la recogida, procesamiento y divulgación de datos, con el fin de conseguir una respuesta efectiva a la pandemia.

[33] The Global Privacy Assembly and The Organization for Economic Co-Operation and Development. "Ensuring data privacy as we battle COVID-19".

Mientras que no deja de ser posible que las medidas excepcionales implementadas en algunos países puedan, en última instancia, resultar ser efectivas a la hora de evitar la propagación del virus, no deja de haber medidas que resultan ser, cuanto menos, controvertidas, en términos de riesgos de vulneraciones de la privacidad de las personas, así como de otros derechos fundamentales de los ciudadanos, particularmente cuando estas medidas no son transparentes ni se informa a los afectados acerca de la existencia de las mismas.

Las autoridades de refuerzo de la privacidad, generalmente, han adoptado una postura pragmática y contextual al respecto, especialmente en tiempos de crisis o de emergencias nacionales, situación similar a la que nos encontramos. En este sentido, han indicado que el respeto fundamental a la protección de datos personales y a la privacidad de las personas no puede interponerse en el camino de medidas necesarias y proporcionadas para el control de la situación provocada por la pandemia.

Los responsables políticos, previa consulta a las autoridades de protección de la privacidad, deben llevar a cabo todos los mecanismos posibles en cuanto a la utilización y el tratamiento de datos durante esta crisis, analizando los riesgos y beneficios que pueda tener cada medida. Sin embargo, han de asegurarse de que cualquier medida extraordinaria que adopten sea proporcional con los riesgos que la misma conlleva, así como de que son implementadas con total transparencia. Igualmente, deberán garantizar que los datos no serán almacenados ni utilizados para otros fines una vez termine la situación de crisis en la que nos encontramos.

b. Otras Instituciones

En cuanto a las otras instituciones que han publicado recomendaciones, si bien no es posible el análisis de todas y cada una de ellas, sí que cabe mencionar que diferentes instituciones de la sociedad civil han publicado informes acerca de la necesidad de respetar la intimidad, la privacidad y los derechos individuales en el tratamiento de los datos para hacer frente a la pandemia provocada por el coronavirus.

Entre ellas destacan el *European Law Institute*, [34] o la carta escrita por la asociación Allai [35] junto con un grupo de profesores universitarios (componiendo un equipo de un total de 58 expertos holandeses) al Primer Ministro (Mark Rutte), los Ministros de Salud, Bienestar y Deporte (Hugo de Jonge, Martin Van Rijn y Feike Sijbesma) y el Ministro de Justicia y Protección Legal (Ferdinand Grapperhaus) de Holanda.

[34] Euopean Law Institute. Principles for the COVID-19 Crisis
[35] Allai. "COVID-19: tracking- and tracing app and healthapp".

## 2. PRINCIPIOS APLICABLES AL TRATAMIENTO DE DATOS PERSONALES

Los datos personales solamente pueden ser recabados atendiendo a las limitaciones legales existentes. Dichas limitaciones o principios, sobre los cuales se asienta la legislación de protección de datos en España, han de ser observados tanto por quienes recopilan datos sensibles como por quienes los tratan.

A continuación, explicaré brevemente en qué consiste cada uno de estos principios.

### 2.1. Principio de calidad de los datos [36]

Este principio es consecuencia de la premisa de la proporcionalidad de los datos, que supone la necesidad de que los datos sean adecuados al propósito que motiva su recopilación.

Los datos de carácter personal solo se podrán recoger para su tratamiento, así como someterlos al mismo, si son adecuados, pertinentes y no excesivos en relación al ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. Igualmente, es necesario que los datos sean exactos y estén actualizados. Dicha situación supone que los datos han de recogerse con un objetivo determinado y, en caso de que posteriormente sean transferidos, es necesario tener en cuenta el objetivo inicial para el cual fueron recopilados.

Asimismo, el art. 6 de la Directiva 95/46/CE señala que el tratamiento de datos ha de hacerse de manera leal y lícita; con fines determinados, explícitos y legítimos, y que los datos no sean tratados posteriormente de manera incompatible con dichos fines. También hace referencia al hecho de que los datos recopilados han de ser adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente.

De esta manera, es posible ver que el principio de calidad de los datos está asentado sobre los pilares de adecuación, finalidad y certeza:

[36] Protección de datos. “Calidad de datos según nuevo reglamento”.

- El principio de adecuación de los datos establece que los datos recogidos han de ser siempre los necesarios para los fines que han de ser tratados. Además, han de estar actualizados, para que las conclusiones a las que llegue el procesador y el tratamiento que reciba el interesado sean correctos.
- La finalidad de los datos supone que los mismos han de servir únicamente a una necesidad concreta. Consecuentemente, no podrán ser utilizados para otra finalidad distinta, salvo en algunos casos concretos en los que se permite el uso secundario de datos.
- El principio de certeza de los datos implica que los datos que se recopilen deben guardar relación con la situación real en la que se encuentre el interesado, ya que esos datos han de ser veraces.

### 2.2. Principio de información y su relación con el principio de transparencia [37]

El principio de información hace referencia tanto al deber como al derecho de información. De esta forma, antes de tratar los datos personales del interesado, habrá que informarle acerca de quién los tratará y con qué finalidad. De esta forma, el interesado estará informado acerca de los datos que se recaban sobre él y será conocedor de quién es su controlador y la meta que quiere alcanzar.

Este principio está íntimamente relacionado con el principio de transparencia, que supone que toda información y comunicación relativa al tratamiento de dichos datos ha de ser fácilmente accesible y entendible para el interesado, por lo que ha de utilizar un lenguaje sencillo y claro. Así, podrá estar perfectamente informado de cuáles son exactamente las ventajas del tratamiento de sus datos, así como de cuales son los inconvenientes que se podrían derivar de dicho tratamiento.

Según el RGPD, el principio de transparencia demanda que "*toda información dirigida al público o al interesado sea concisa, fácilmente accesible y fácil de entender, y que se utilice un lenguaje claro y sencillo, y, además, en su caso, se visualice. Esta información*

[37] Iberley. "Principio de transparencia en el Reglamento general de protección de datos (RGPD) y en la LO 3/2018 (LOPDGDD)".

*podría facilitarse en forma electrónica, por ejemplo, cuando esté dirigida al público, mediante un sitio web. Ello es especialmente pertinente en situaciones en las que la proliferación de agentes y la complejidad tecnológica de la práctica hagan que sea difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad, datos personales que le conciernen, como es en el caso de la publicidad en línea".* Considerando 58 del RGPD

Además, el considerando 39 de la citada norma europea expone que el principio de transparencia requiere que *"toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Dicho principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento. Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales así como del modo de hacer valer sus derechos en relación con el tratamiento. En particular, los fines específicos del tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de su recogida".*

Es decir, el citado principio se refiere, en concreto, a aspectos como:

- La información de los interesados sobre la identidad del responsable del tratamiento.
- Los fines del tratamiento.
- La información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas.
- El derecho a obtener la confirmación y comunicación de los datos personales que les conciernan y que sean objeto de tratamiento.

## 2.3. Principio de consentimiento del afectado y su relación con el principio de licitud del tratamiento [38]

El consentimiento consiste en la manifestación libre, voluntaria y consciente del interesado. Para que sea válido, además, ha de ser otorgado en pleno uso de sus facultades mentales después de recibir la información necesaria.

Para que sea válido, el consentimiento ha de cumplir una serie de requisitos:

- Libre: para que el consentimiento sea otorgado libremente, deberá haber sido obtenido en ausencia de vicios del consentimiento.
- Específico: ha de estar referido a una finalidad específica y legítima, de tal forma que no cabe un consentimiento genérico.
- Informado: el interesado ha de ser conocedor, antes de proceder al tratamiento de sus datos, la existencia de la recopilación y las finalidades para las que se produce.

Por su parte, el principio de licitud del tratamiento supone una ampliación a las bases legítimas para el tratamiento de datos establecidas en el RGPD.
Este principio supone que será lícito el tratamiento de datos con fines distintos a aquel con el que se habían recabado inicialmente, siempre que el nuevo fin sea muy similar al primero.

Para determinar dicha similitud, es necesario atender a criterios como la relación que existe entre los fines, el contexto en el que se recabaron, la naturaleza de los datos, la consecuencia que el nuevo tratamiento tiene para los interesados y la existencia de garantías adecuadas.

De esta manera, el consentimiento es la base legítima aplicable a la mayoría de tratamientos de datos, pero no es la única. Consecuentemente, determinados tratamientos podrán tomar como base otras que también sean legítimas, como el caso de cumplimiento de obligaciones legales. Así, no existe un único modo de prestar el consentimiento, sino que puede adoptar diferentes formas siempre que se respeten los principios legalmente establecidos.

---

[38] García del Poyo, R. *Big Data: Regulación y uso secundario de datos, circulación de datos no personales. Suministro de contenidos y comercio electrónico*

En el caso concreto de las obligaciones respecto al uso secundario de datos e información del Sector Público existen, además una serie de obligaciones adicionales:

El art. 13.3 RGPD exige que cualquier finalidad ulterior prevista por el responsable del tratamiento para los datos personales de un interesado sea informada antes de comenzar el tratamiento, independientemente de la base de legitimación aplicable.

Del mismo modo, debe informarse, entre otras cosas, de los derechos que asisten a los interesados, de manera que estos puedan ejercitarlos si así lo consideran oportuno (por ejemplo, en el caso de que un interesado se oponga a que se utilicen sus datos para investigaciones basadas en el interés legítimo del responsable del tratamiento).

La reutilización de la información del sector público que pueda contener datos personales queda sujeta a la Ley 37/2007, de 16 de noviembre, sobre Reutilización de la Información del Sector Público.

Asimismo, el art. 15 de la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno determina que "*en los supuestos en que se pretenda el acceso a información que contenga datos de carácter personal, solo se podrá estimar la solicitud previa ponderación suficientemente razonada del interés público en la divulgación de información y los derechos de los afectados cuyos datos aparezcan en la información solicitada*".

### 2.4. Principio de proporcionalidad [39]

El principio de proporcionalidad puede ser entendido desde tres puntos de vista: ponderación (de la medida se derivan más beneficios que perjuicios para otros bienes o valores que pudiesen entrar en conflicto), idoneidad (la medida es susceptible de alcanzar el objetivo propuesto) y necesidad (no existe otra medida más moderada para conseguir el mismo objetivo con la misma eficacia).

[39] Perello Domenech, I. "El principio de proporcionalidad y la jurisprudencia constitucional". *Dialnet*

## 2.5. Principio de limitación de la finalidad [40]

Una de las definiciones más aceptadas del principio de limitación de la finalidad es dada por parte de la AEPD. Este principio implica, por una parte, la obligación de que los datos sean tratados con una o varias finalidades determinadas, explícitas y legítimas y, por otra, que se prohíbe que los datos recogidos con unos fines determinados, explícitos y legítimos sean tratados posteriormente de una manera incompatible con esos fines.

## 2.6. Principio de interés legítimo

El interés legítimo es uno de los fundamentos para la licitud del tratamiento de datos personales, como indica el art. 6.1 f) del RGPD. Sin embargo, es necesario delimitar el alcance de dicho concepto para que no permita que cualquier entidad realice actividades de recopilación y tratamiento de datos sin las condiciones necesarias para justificarlas.

La actual Ley Orgánica de Protección de Datos y garantía de derechos digitales no incluye una regla concreta sobre esta materia, pero sí asume la doctrina del Consejo de Estado, regulando en su Título IV diversos supuestos que constituyen presunciones legales de prevalencia del interés legítimo.

Algunos de los criterios que se pueden utilizar son:

- El impacto que dicho tratamiento tenga en el interesado.
- La naturaleza de los datos objeto de tratamiento.
- La forma de dicho tratamiento.
- Las expectativas razonables de los interesados en relación con el tratamiento.
- El desequilibrio entre el responsable del tratamiento y el interesado.

[40] AEPD. “Principios”.

## CAPÍTULO III. LA CONCRETA APLICACIÓN EN TELÉFONOS MÓVILES

Como indicaba al principio del trabajo, para facilitar la solución del problema que la pandemia del COVID-19 está causando, la solución propuesta consiste en el desarrollo de una aplicación para teléfonos móviles.

Para ello, es necesario analizar la situación en la que se encuentran otras aplicaciones que recogen datos, las partes del contrato cuando un usuario descarga una aplicación de esas características, la adaptación de los principios generales del campo de la Protección de Datos a nuestra aplicación y las garantías legales existentes acerca del uso secundario de datos.

### 1. LA RECOGIDA DE DATOS POR PARTE DE LAS APLICACIONES DE LOS TELÉFONOS MÓVILES

No existe duda ninguna acerca de la importancia que los teléfonos móviles tienen en nuestra vida diaria. Prácticamente todas las personas tenemos más de un dispositivo inteligente, siempre con un gran abanico de aplicaciones descargadas en él, para maximizar al máximo nuestra experiencia de usuario.

Muchas de estas aplicaciones pueden ser descargadas por parte del usuario sin efectuar el pago de ninguna cantidad económica. Sin embargo, como indica FERNÁNDEZ ACEVEDO [41], los desarrolladores de estas aplicaciones compensan dicha gratuidad con la información que obtienen del usuario que las descarga.

El Dictamen 02/2013 [42] hace referencia a los riesgos que existen para los usuarios a raíz de estas aplicaciones en los teléfonos móviles. Dicho Dictamen destaca principalmente la falta de transparencia y de consentimiento libre, informado y previo, aunque también hace referencia a las insuficientes medidas de seguridad que el desarrollador de la aplicación impone y el incumplimiento del principio de limitación de la finalidad que realiza.

[41] Fernández Acevedo, J. "Redes sociales y aplicaciones móviles"
[42] Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes

## 2. PARTES DEL CONTRATO

### 2.1. Fabricantes de teléfonos móviles

Es importante tenerlos en cuenta también porque muchos de los datos personales a los que tienen acceso las aplicaciones que el usuario se descarga provienen de su teléfonos móviles.

Tienen también la consideración de responsables del tratamiento, ya que determinan los instrumentos que las aplicaciones pueden utilizar para acceder a los datos que se encuentran en el teléfono móvil del usuario que las descarga.

### 2.2. Tiendas de aplicaciones

Cada dispositivo móvil tiene su tienda de aplicaciones propia (Apple Store, Play Store…) a través de la cual el usuario puede descargar todas las aplicaciones que ofrece.

Las tiendas de aplicaciones también son responsables del tratamiento, ya que disponen de información acerca del usuario, quien es obligado a introducir una serie de datos cuando se registra en la tienda.

MARÍN LÓPEZ [43] sintetiza las medidas que las tiendas han de cumplir. No son solo relativas al tratamiento y la protección de los datos del usuario, sino que también han de facilitarle mecanismos de desinstalación sencillos.

### 2.3. Desarrollador de la aplicación

Dentro de este concepto se incluyen tanto los creadores de las aplicaciones como las empresas que los subcontratan.

---

[43] Marín López, J. "La protección de datos en las aplicaciones de los dispositivos Inteligentes". *Gómez-Acebo y Pombo*

Según el Dictamen 02/2013 mencionado previamente, son responsables del tratamiento. Esta consideración se debe a que son los encargados de decidir tanto la finalidad como los mecanismos utilizados para el tratamiento. De esta manera, deberán acotar los datos a los que la aplicación tendrá acceso una vez descargada.

Además, el art. 35.1 RGPD indica que "*Cuando sea probable que un tipo de tratamiento, en particular, si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará antes del tratamiento una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales*".

Ya que las tecnologías utilizadas podrían resultar de lato riesgo para los derechos y libertades de las personas físicas, los desarrolladores de la aplicación habrán de realizar la evaluación del impacto.
El art. 35.7 RGPD indica los contenidos mínimos de dicha evaluación del impacto.

*"La evaluación deberá incluir como mínimo:*

*a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;*

*b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;*

*c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y*

*d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas."*

## 3. PRINCIPIOS APLICABLES

### 3.1. Principio de licitud del tratamiento

En términos generales, el principio de licitud del tratamiento supone una ampliación a las bases legítimas para el tratamiento de datos establecidas en el RGPD.
Este principio supone que será lícito el tratamiento de datos con fines distintos a aquel con el que se habían recabado inicialmente, siempre que el nuevo fin sean muy similar al primero.

Para determinar dicha similitud, es necesario atender a los criterios establecidos en el artículo 6.1 RGPD. Dentro de los mismos, nos encontramos con la relación que existe entre los fines, el contexto en el que se recabaron, la naturaleza de los datos, la consecuencia que el nuevo tratamiento tiene para los interesados y la existencia de garantías adecuadas.

En cuanto a la situación de nuestra aplicación para teléfonos móviles, el requisito principal es que los datos personales del interesado no sean tratados sin su consentimiento.

El tratamiento de los datos personales del interesado puede realizarse bien gracias a su consentimiento explícito, como establecía el principio de consentimiento del afectado, o bien gracias a alguna otra de las bases legítimas establecidas en el artículo 6.1 RGPD.

### 3.2. Principio de limitación de la finalidad y principio de minimización de datos

El principio de limitación de la finalidad supone, en términos generales, que los datos han de ser tratados con una finalidad determinada, explícita y legítima. Consecuentemente, quedaría prohibido un tratamiento posterior en cumplimiento de otro objetivo distinto.

El principio de minimización de datos exige que los datos personales han de ser "*adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados*", según indica el art. 5.1 c) del RGPD.

En el caso concreto de la aplicación para el teléfono móvil, la aplicación de estos principios supondría que los datos recogidos solamente pueden ser tratados para el cumplimiento de una finalidad concreta. Además, la recopilación ha de hacerse únicamente de los datos que sean estrictamente necesarios para alcanzar ese propósito.

### 3.3. Principio de interés legítimo

El interés legítimo es uno de los fundamentos que permiten la licitud del tratamiento de datos personales. Sin embargo, no existe una definición del concepto en la normativa jurídica.

Analizando la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y garantía de derechos digitales, el Título IV establece una serie de disposiciones aplicables a tratamientos concretos basadas en el concepto de interés legítimo. En este sentido, existen presunciones iuris tantum acerca de la existencia de interés legítimo.

Consecuentemente, en casos distintos a los indicados en dicho Título IV, será el controlador de datos quien deba probar la existencia de interés legítimo para llevar a cabo la recogida de datos.

## 4. USO SECUNDARIO DE DATOS

Según GARCÍA DEL POYO [44], el uso secundario puede definirse como "la utilización de datos para una finalidad distinta de aquella para la que fueron recabados inicialmente". Este tratamiento se utiliza fundamentalmente en el ámbito de la investigación médica, por lo que sería extrapolable a nuestra aplicación.
Dependiendo de las características del tratamiento, dichos datos pueden considerarse como:

- Datos personales: incluso aquellos que sean seudonimizados o disociados, si es posible la re-identificación. En este sentido, es necesario tener en cuenta que los datos en el ámbito de la investigación médica podrían considerarse categorías especiales de datos personales.

[44] García del Poyo, R. *Big Data: Regulación y uso secundario de datos, circulación de datos no personales. Suministro de contenidos y comercio electrónico*

- Datos no personales: únicamente si los datos han sido irreversiblemente anonimizados

El uso secundario de datos, por tanto, está íntimamente relacionado con el principio de licitud del tratamiento. De esta forma, será lícito el tratamiento de datos con fines distintos a aquel con el que se habían recabado inicialmente, siempre que el nuevo fin sea muy similar al primero.

Para determinar dicha similitud, es necesario atender a criterios como la relación que existe entre los fines, el contexto en el que se recabaron, la naturaleza de los datos, la consecuencia que el nuevo tratamiento tiene para los interesados y la existencia de garantías adecuadas.

## CAPÍTULO IV. CONCLUSIONES

Una vez realizado el análisis del régimen legal aplicable en materia de protección de datos a una aplicación de rastreo telefónico, así como las cuestiones técnicas relacionadas con el big data y el entorno legal en el que se encuentra el ámbito de protección de datos, resulta procedente la recopilación de las conclusiones obtenidas.

En primer lugar, resulta obvio que la implementación de técnicas de big data puede contribuir tanto en el medio como en el largo plazo a mejorar la prevención de enfermedades y epidemias, así como el tratamiento de los pacientes. Además, será posible tanto que la gestión sanitaria esté dotada de más agilidad como que los beneficios económicos que la misma genera se vean incrementados, principalmente como consecuencia de la reducción de costes sanitarios.

En relación con lo anterior, es necesario contar con instrumentos de carácter tecnológico para que sea posible no solo la recogida y almacenamiento seguro de los datos, sino también un trato eficaz de los mismos. Actualmente, como la gestión de la pandemia derivada del COVID-19 ha demostrado, no contamos con los mecanismos suficientes para hacer frente a una pandemia.

En segundo lugar, una vez analizada la necesidad de contar con herramientas tecnológicas, resulta procedente el estudio de cuál es el régimen legal aplicable a las mismas. En este sentido, tanto el RGPD como la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales coinciden con las agencias europeas de protección de datos acerca de la aplicación de una serie de principios como garantías legales del mencionado tratamiento. Estos principios se refieren tanto al tipo de datos que se recogerán (calidad de los datos) como al interesado cuyos datos se recogen (información, transparencia, licitud del tratamiento…) y el propósito de dicha recogida (limitación de la finalidad).

Por último, respecto a las garantías legales que la aplicación debería cumplir, resulta destacable el hecho de que ya existen numerosas aplicaciones que recogen datos de teléfonos móviles. Consecuentemente, tanto los desarrolladores de la aplicación como las tiendas a través de la cual el usuario las descarga, así como los fabricantes del teléfono

móvil, se convierten en responsables del tratamiento de datos. Además, dicho tratamiento ha de respetar una serie de principios, vinculados tanto con la meta que se quiere alcanzar con el tratamiento (interés legítimo y limitación de la finalidad) como con el grado de consentimiento que el interesado ha de prestar (licitud del tratamiento).

**ANEXO**

1. RESUMEN ORIGINAL DE "GUIDELINES 03/2020 ON THE PROCESSING OF DATA CONCERNING HEALTH FOR THE PURPOSE OF SCIENTIFIC RESEARCH IN THE CONTEXT OF THE COVID-19 OUTBREAK".

   The guidelines on the processing of health data for research purposes in the context of the COVID-19 outbreak aim to shed light on the most urgent legal questions concerning the use of health data, such as the legal basis of processing, further processing of health data for the purpose of scientific research, the implementation of adequate safeguards and the exercise of data subject rights.

   The guidelines state that the GDPR contains several provisions for the processing of health data for the purpose of scientific research, which also apply in the context of the COVID-19 pandemic, in particular relating to consent and to the respective national legislations. The GDPR foresees the possibility to process certain special categories of personal data, such as health data, where it is necessary for scientific research purposes.

   In addition, the guidelines address legal questions concerning international data transfers involving health data for research purposes related to the fight against COVID-19, in particular in the absence of an adequacy decision or other appropriate safeguards.

   Andrea Jelinek, Chair of the EDPB, said: "Currently, great research efforts are being made in the fight against COVID-19. Researchers hope to produce results as quickly as possible. The GDPR does not stand in the way of scientific research, but enables the lawful processing of health data to support the purpose of finding a vaccine or treatment for COVID-19".

2. RESUMEN ORIGINAL DE "GUIDELINES 04/2020 ON THE USE OF LOCATION DATA AND CONTACT TRACING TOOLS IN THE CONTEXT OF THE COVID-19 OUTBREAK".

The guidelines on geolocation and other tracing tools in the context of the COVID-19 outbreak aim to clarify the conditions and principles for the proportionate use of location data and contact tracing tools, for two specific purposes:

1. using location data to support the response to the pandemic by modelling the spread of the virus in order to assess the overall effectiveness of confinement measures;

2. using contact tracing, which aims to notify individuals who may have been in close proximity to someone who is eventually confirmed as a carrier of the virus, in order to break the contamination chains as early as possible.

The guidelines emphasise that both the GDPR and the ePrivacy Directive contain specific provisions allowing for the use of anonymous or personal data to support public authorities and other actors at both national and EU level in their efforts to monitor and contain the spread of COVID-19. The general principles of effectiveness, necessity, and proportionality must guide any measures adopted by Member States or EU institutions that involve processing of personal data to fight COVID-19.

The EDPB stands by and underlines the position expressed in its letter to the European Commission (14 April) that the use of contact tracing apps should be voluntary and should not rely on tracing individual movements, but rather on proximity information regarding users.

Dr. Jelinek added: “Apps can never replace nurses and doctors. While data and technology can be important tools, we need to keep in mind that they have intrinsic limitations. Apps can only complement the effectiveness of public health measures and the dedication of healthcare workers that is necessary to fight COVID-19. At any rate, people should not have to choose between an efficient response to the crisis and the protection of fundamental rights.”

In addition, the EDPB adopted a guide for contact tracing apps as an annex to the guidelines. The purpose of this guide, which is non-exhaustive, is to provide general guidance to designers and implementers of contact tracing apps, underlining that any assessment must be carried out on a case-by-case basis.

3. RESUMEN ORIGINAL DE “JOINT STATEMENT ON THE RIGHT TO DATA PROTECTION IN THE CONTEXT OF THE COVID-19 PANDEMIC”.

While it is crucial to make clear that data protection can in no way be an obstacle to save human lives, it is equally crucial to reaffirm that the exercise of human rights, and notably the rights to privacy and to data protection are still applicable. Data protection principles always allow for balancing the interests at stake. Convention 108+ sets forth high standards for the protection of personal data which are compatible and reconcilable with other fundamental rights and relevant public interests.

The principles enshrined in several international and national instruments cannot be suspended but only restricted in a lawful manner, and so for a defined limited duration.

Since massive data and data bases are generated, seizing the benefits of data processing techniques and technologies such as Big Data or Artificial Intelligence, that data should be processed in such environments in a way that respects human dignity and data protection. The respective guidance developed by the Committee of Convention 108 in the context of Big Data and Artificial Intelligence can be useful tools for developers as well as governments to shape those processing in a way that safeguards against voluntary misuse or unintended negative consequences, including the discrimination of individuals or groups of individuals.

Transparency and “explainability” of analytics or AI solutions, a precautionary approach and a risk management strategy (including the risk of re-identification in the case of anonymised data), a focus on data quality and minimisation, and the role of human oversight are some of the key points to take into account in the development of innovative solutions to fight against COVID-19.

**BIBLIOGRAFÍA**

1. DOCTRINA

García del Poyo, R. *Big Data: Regulación y uso secundario de datos, circulación de datos no personales. Suministro de contenidos y comercio electrónico*. Madrid, 2020

Nass, S. J., Levit, L. A., & Gostin, L. O. (Eds.). (2009). "Beyond the HIPAA Privacy Rule". *Institute of Medicine*. Published. (disponible en https://doi.org/10.17226/12458; última consulta 4/06/2021).

O'Driscoll, A., Daugelaite, J., & Sleator, R. D. (2013). "'Big data', Hadoop and cloud computing in genomics". *Journal of Biomedical Informatics, 46*(5), 774–781. (disponible en: https://doi.org/10.1016/j.jbi.2013.07.001; última consulta 4/06/2021)

Llácer Matacás, MªR., Casado, M., BUISAN ESPELETA, L. *Documento sobre bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública*. Observatori de Bioètica i Dret, Universidad de Barcelona Publicacions i Edición. Barcelona, 2015.

Gil González, E. *Big Data, privacidad y protección de datos. Agencia Española de Protección de Datos*. Madrid, 2016

Calvo, L. J., Varela, A. B., Rigaudias, Á. C., & Fernández, J. (2019). *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD* (1.ª ed.). BOSCH.

Marín López, J. "La protección de datos en las aplicaciones de los dispositivos Inteligentes". *Gómez-Acebo y Pombo*. (disponible en https://www.ga-p.com/wp-content/uploads/2018/03/la-proteccion-de-datos-en-las-aplicaciones-de-los-dispositivos-inteligentes.pdf; última consulta 05/06/2021)

Perello Domenech, I. "El principio de proporcionalidad y la jurisprudencia constitucional". *Dialnet*

Fernández Acevedo, J. “Redes sociales y aplicaciones móviles” en López Calvo, J. (coord.) *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos*, Wolters Kluwer, Madrid, 2018, pp 223-248.

## 2. LEGISLACIÓN

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. (BOE 14 de diciembre de 1999)

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. (BOE 6 de diciembre de 2018).

Reglamento General de Protección de Datos 2016/679 (Parlamento Europeo y Consejo de la Unión Europea, de 27 de abril de 2016)

Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes (Diario oficial de la Unión Europea 27 de febrero de 2013)

Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público. (BOE 17 de noviembre de 2007)

Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. (BOE 10 de diciembre de 2013)

## 3. REFERENCIAS DE INTERNET

### 3.1. Agencias de Protección de Datos

Agencia Española de Protección de Datos. Página web oficial. (disponible en: https://www.aepd.es/es; última consulta 10/06/2021)

European Data Protection Board. Página web oficial. (disponible en:

https://edpb.europa.eu/edpb_en; última consulta 11/06/2021)

European Data Protection Board. Sección COVID. (disponible en: https://edpb.europa.eu/search/site/COVID_en; última consulta 10/11/2020)

Eur-Lex. El acceso al Derecho de la Unión Europea. (disponible en: https://eur-lex.europa.eu/homepage.html?locale=es; última consulta 11/11/2020)

Consejo de Europa en materia de Protección de Datos. Página web. (disponible en: https://www.coe.int/es/web/data-protection; última consulta 12/11/2020)

Consejo de Europa en materia de Protección de Datos en el ámbito del COVID-19. Página web. (disponible en: https://www.coe.int/es/web/data-protection/covid-19-data-protection; última consulta 1/12/2020)

Asamblea Global de Privacidad y OECD. Página web oficial. (disponible en: https://globalprivacyassembly.org/; última consulta 12/12/2020)

Asamblea Global de Privacidad y OECD. Repositorio de recomendaciones de instituciones oficiales en protección de datos durante la pandemia de COVID-19. (disponible en: https://globalprivacyassembly.org/covid19/covid19-resources/; última consulta 15/12/2020)

Agencia Española de Protección de Datos. "Informe sobre el tratamiento de datos personales en relación con la situación derivada de la extensión del virus COVID-19". (disponible en: https://www.aepd.es/es/documento/2020-0017.pdf; última consulta 16/12/2020)

Agencia Española de Protección de Datos. "El uso de las tecnologías en la lucha contra el COVID-19. Un análisis de costes y beneficios". (disponible en: https://www.aepd.es/sites/default/files/2020-05/analisis-tecnologias-COVID19.pdf; última consulta 18/12/2020)

Agencia Española de Protección de Datos. Webinario "Innovación, protección de datos y salud (I). Soluciones tecnológicas para combatir el COVID-19". (disponible en: https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/webinario-innovacion-pd-y-salud-I; última consulta 19/12/2020)

Agencia Española de Protección de Datos. Webinario 'Innovación, protección de datos y salud (II)'. Bioética y Derecho. Proteger la privacidad en la sociedad digital post COVID-19. (disponible en: https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/acceso-webinario-innovacion-pd-y-salud-II; última consulta 10/01/2021).

European Data Protection Board. Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak. (disponible en: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf; última consulta 15/01/2021).

European Data Protection Board. Guidelines 04/2020 on the use of location data and contract tracing tools in the context of the COVID-19 outbreak. (disponible en: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf; última consulta 17/01/2021).

Comisión Europea. Recomendación 2020/518. (disponible en: https://eurlex.europa.eu/legalcontent/ES/TXT/PDF/?uri=CELEX:32020H0518&from=EN; última consulta 19/01/2021).

Comisión Europea. Comunicación 124/I/01. (disponible en: https://eurlex.europa.eu/legalcontent/ES/TXT/PDF/?uri=CELEX:52020XC0417(08)&from=EN; última consulta 23/01/2021).

Consejo de Europa. "Joint Statement on the right to data protection in the context of the COVID-19 pandemic". (disponible en: https://rm.coe.int/covid19-joint-statement/16809e09f4; última consulta 01/02/2021).

The Global Privacy Assembly and The Organization for Economic Co-Operation and Development. “Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics”. (disponible en: https://globalprivacyassembly.org/wpcontent/uploads/2020/05/PolicyNote_TrackingTracingCovid_FINAL.pdf; última consulta 03/02/2021)

The Global Privacy Assembly and The Organization for Economic Co-Operation and Development. “Ensuring data privacy as we battle COVID-19”. (disponible en: https://globalprivacyassembly.org/wpcontent/uploads/2020/05/PolicyNote_Covid_DataPrivacy_FINAL.pdf; última consulta 05/02/2021).

The Global Privacy Assembly and The Organization for Economic Co-Operation and Development. Repositorio de recomendaciones de instituciones oficiales en protección de datos durante la pandemia de COVID-19. (disponible en: https://globalprivacyassembly.org/covid19/covid19-resources/; última consulta 06/02/2021).

Euopean Law Institute. Principles for the COVID-19 Crisis. (disponible en: https://rm.coe.int/european-law-institure-principles-for-covid-19-crisis/16809e83bb; última consulta 10/02/2021).

Allai. “COVID-19: tracking- and tracingapp and healthapp”. (disponible en: http://allai.nl/wp-content/uploads/2020/04/Online-version-Letter-to-President-Rutte-Ministers-De-Jonge-Van-Rijn-Grapperhaus-re.-COVID-19-apps.pdf; última consulta 16/02/2021)

### 3.2. Otros

“Obama Administration Unveils “BIG DATA” Initiative: Announces $200 Million in New R&D Investments”, *IEEE Signal Processing Society*, 1 de agosto de 2017.

(disponible en: https://signalprocessingsociety.org/newsletter/2012/04/obama-administration-unveils-%E2%80%9Cbig-data%E2%80%9D-initiative-announces-200-million-new-rd; última consulta 01/06/2021)

Siemens. "*Healthcare Dives into Big Data"*. (disponible en: https://www.siemenshealthineers.com/en-us/news-and-events/mso-big-data-and-healthcare-1; última consulta 02/06/2021)

Cottle, M., Kanwal, S., Kohn, M., Strome, T., & Treister, N. "Transforming health care through Big Data". *Institute for health technology transformation*. (disponible en: http://c4fd63cb482ce6861463-bc6183f1c18e748a49b87a25911a0555.r93.cf2.rackcdn.com/iHT2_BigData_2013.pdf; última consulta 03/06/2021)

Ishwarappa, & Anuradha, J. "A brief introduction on Big Data 5Vs Characteristics and Hadoop Technology". *Procedia Computer Science 48*. (disponible en: https://www.sciencedirect.com/science/article/pii/S1877050915006973; última consulta 04/06/2021)

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., & Byers, A. H. "Big data: The next frontier for innovation, competition, and Productivity". *McKinsey & Company*. (disponible en: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/big-data-the-next-frontier-for-innovation; última consulta 05/06/2021)

Roski J, Bo-Linn GW, Andrews TA. Creating value in health care through big data: opportunities and policy implications. *Health Affair*. (disponible en: doi: 10.1377/hlthaff.2014.0147; última consulta 4/06/2021)

Curtis, J. "NHS boss claims patient data collection is «morally right»". *IT PRO*. (disponible en:

https://www.itpro.co.uk/public-sector/23844/nhs-boss-claims-patient-data-collection-is-morally-right; última consulta 07/06/2021)

AQuAS, A. "El proyecto VISC+ es una oportunidad para la mejora de la calidad de la atención sanitaria". *AQuAS Blog*. (disponible en: https://blog.aquas.cat/2015/02/26/el-proyecto-visc-es-una-oportunidad-para-la-mejora-de-la-calidad-de-la-atencion-sanitaria/?lang=es; última consulta 07/06/2021)

Planas, J. "BIG DATA Revolución en el sector sanitario - Dr. Jorge Planas*". Dr. Jorge Planas Blog Personal*. (Disponible en: https://www.clinicaplanas.com/jorge-planas/2012/10/29/big-data-la-proxima-revolucion-en-el-sector-sanitario-jorge-planas/; última consulta 08/06/2021).

Rodrigo Larrucea, C. "Mhealth y Bigdata en sanidad". *Derecho y Salud no van siempre de la mano*. (Disponible en: https://carmenrodrigodelarrucea.wordpress.com/2016/04/14/mhealth-y-bigdata-en-sanidad/#more-793; última consulta 08/06/2021).

Fundación Instituto Roche – "III Jornada «Hacia un Sistema Sanitario basado en la creación de Valor". *El médico interactivo*. (Disponible en: https://www.institutoroche.es/jornadas/70-3a-jornada-hacia-un-sistema-sanitario-basado-en-la-creacion-de-valor-la-era-de-los-datos-nuevo-paradigma-en-la-financiacion-de-farmacos-innovadores; última consulta 10/06/2021)

Calderón, P. C. L. "Big data en sanidad en España: la oportunidad de una estrategia nacional". *Parra Calderón*. (Disponible en: https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S0213-91112016000100013; última consulta 10/06/2021).

Protección de datos. "Calidad de datos según nuevo reglamento". (Disponible en: https://www.protecciondatos.org/calidad-de-datos/; última consulta 11/06/2021).

Iberley. "Principio de transparencia en el Reglamento general de protección de datos (RGPD) y en la LO 3/2018 (LOPDGDD)". (Disponible en:

https://www.iberley.es/temas/principio-lealtad-transparencia-rgpd-lopdgdd-62721; última consulta 11/06/2021).

AEPD. “Principios”. (Disponible en: https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/principios ; última consulta 11/06/2021).