
Universidad de Valladolid

**Facultad de Ciencias Sociales, Jurídicas y de la Comunicación**

**Grado en Derecho.**

# TRABAJO FIN DE GRADO: GEOLOCALIZACIÓN DE LAS PERSONAS FÍSICAS EN EL CONTEXTO DE LA PANDEMIA POR LA COVID – 19.

**Autora: Sara Sanz Guedán**

**Tutora de TFG: Isabel Palomino Diez**

**Curso 2020 - 2021**

*Dedicado a aquellas personas que*
*creyeron en mí cuando ni yo misma lo hacía.*

# ÍNDICE

## RESUMEN:

Este año ha estado marcado tanto por la pandemia originada por el Sars-Cov-2, como por el avance tecnológico. La geolocalización es un punto muy importante dentro de las redes sociales, que, en la actualidad, han pasado a formar parte indispensable en nuestro día a día, ya sea para el trabajo, como para relacionarnos con nuestra familia o amigos.

Pero todo tiene un precio en cuanto a una privacidad e intimidad, por lo que debemos conocer cómo, cuándo y por qué se adquieren nuestros datos de los dispositivos que utilizamos, y qué se hacen con ellos; pero lo más importante, es tener conocimiento de hasta qué punto tienen, tanto los fabricantes como otros sujetos, para utilizar nuestros datos y/o búsquedas con un fin comercial, y por supuesto, que los datos que recaben sean acordes al fin que quieren conseguir y no superen los límites regulados.

## Palabras clave:

Geolocalización, datos personales, Derecho a la Intimidad, Derecho a la Privacidad, redes sociales, Radar Covid.

## ABSTRACT:

This year has been marked by the covid 19 pandemic and the associated technological advancements. There is a very important point in Social Media, especily, nowadays that it has started to be an indispensable part in our day a day, either in work or in our interaction with our family and friends.

However everything has a price, so we need to know how, when and why our data is needed from us. The most important thing is to have the knowledge of what can and will of be asked of manufacturers and the subjects, use our data and/or search results for a comercial purpose, and of course, that the data that they collect is in accordance with the purpose that they describe and that it does not exceed regulations in the given country.

## Keywords:

Geolocation, personal data, Right to Privacy, Right to Privacy, Social Networks, Covid Radar.

## ABREVIATURAS

AAPP..... Administraciones Públicas.

AEPG..... Agencia Española de Protección de Datos.

CC..... Código Civil.

CE..... Constitución Española.

CP..... Código Penal.

ET..... Estatuto de los Trabajadores.

GPS..... Sistema de Posicionamiento Global.

LISSI..... Ley 34/2002, de 11 de julio, de Servicio de la Sociedad de la Información y del Comercio Electrónico.

LOPDGDD..... Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

RGPD..... Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

RLOPD..... Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

STS..... Sentencia Tribunal Supremo.

TIC..... Tecnologías de la Información y la Comunicación.

# 1. INTRODUCCIÓN.

El 2020 ha estado marcado por dos hechos fundamentales, la pandemia originada por el Covid-19 y el avance tecnológico. Como consecuencia de la declaración del Estado de Alarma en marzo, por el que se nos confinaba a la población en nuestros domicilios durante un periodo de tres meses, nos hemos visto abocados a utilizar en exceso las tecnologías, ya sea para el teletrabajo, para impartir clase a todos los estudiantes, o simplemente para comunicarnos con nuestros amigos.

Al involucrarnos tanto en las tecnologías, hubo un momento en el que dejamos de lado nuestra vida física al tener una digital. Esto se explica porque todos nosotros necesitamos conectarnos a la red para realizar cualquier tipo de trabajo. Por ello, hemos podido comprobar que en la actualidad el teletrabajo se ha convertido en una figura fundamental dentro de nuestro sistema laboral, pero también las Redes sociales, por las que los jóvenes, y no tan jóvenes, nos hemos ido comunicando en nuestro periodo de confinamiento para así amenizar el tiempo y poder distraernos de la realidad.

Atendiendo al argumento que defiende PÉREZ LUCO[1], *lo que nadie discute es que la revolución tecnológica está produciendo unos cambios en el comportamiento de los individuos y de los grupos sociales, que implican una remodelación de la imagen del hombre en el universo.*

Al involucrarnos tanto en las Redes sociales, creamos un mundo ficticio donde mostramos lo que nosotros queremos que otros vean, pero todo ello se aleja de la realidad. Olvidamos que, al exponernos a este nivel, perdemos nuestra privacidad, nuestro pequeño derecho a la intimidad donde nosotros somos los dueños de nuestros datos; es aquí donde entran en conflicto las nuevas tecnologías y nuestro derecho a la vida privada o el derecho a la intimidad.

Para entender mejor la diferencia entre intimidad y privacidad tendremos que comparar ambos conceptos con las estancias de una casa. Por una parte, la intimidad se podrá equiparar con el dormitorio o el cuarto de baño, mientras que la privacidad es un concepto más extenso, por lo que podría ser el salón y la cocina; entendemos que estas estancias de la casa no son tan íntimas, pero sí son privadas.

[1] PÉREZ LUÑO, Antonio-Enríquez. *Nuevas tecnologías, sociedad y derecho: el impacto socio-jurídico de las N.T. de la información*. Colección Impactos, 1ª E., Madrid, Fundesco, 1987, pp. 154. Pág. 21.

En este mundo "virtual", regulado por el Derecho interno y europeo, como veremos en próximos epígrafes, las personas físicas son equiparadas a datos, y la disponibilidad e interconexión de la información que se recolecta de sus dispositivos, se manipula para conocer de sus gustos y aficiones.

Cuando hablamos de Redes sociales indiscutiblemente tenemos que mencionar la geolocalización; ésta es una herramienta que permite ubicar un dispositivo en un punto espacial a partir de la transmisión de sus coordenadas de posicionamiento[2]. Por consiguiente, con esta herramienta lo que se consigue es localizar la ruta de una población, determinar su lugar en el mapa de coordenadas, insertar las coordenadas exactas del lugar donde se tomó una fotografía, remitir publicidad a nuestro teléfono u ordenador de las búsquedas que hayamos realizado, o incluso, en muchos sitios web, es imprescindible activar nuestra localización para acceder a ellos.

La desventaja de la utilización de la geolocalización sería el uso abusivo de nuestra intimidad, porque los usuarios de terminales electrónicos los llevamos siempre con nosotros y, por lo tanto, siempre estaremos localizados, con unos datos exhaustivos de nuestra dirección.

Como explica BARINAS UBIÑA[3], la geolocalización propicia la confección de "*perfiles y patrones de comportamiento que van horadando las barreras de lo que representa la idea de privacidad desde una reconfiguración de la identidad y personalidad del ser humano, ahora representada, dentro de este entorno digital, a través de datos que se interconectan*".

Por consiguiente, dentro de este nuevo mundo de interacción, nos preguntamos cómo quedarán protegidos los derechos y libertades fundamentales, en especial, la vida privada, frente a las amenazas que las nuevas tecnologías puedan suponer para ella.

Nos tenemos que preguntar, por tanto, ¿nos hemos convertido en meros datos para las Redes sociales? ¿Hemos traspasado la frontera entre el mundo "físico" a un mundo "virtual"?

---

[2] BATUECAS CALETRÍO, Alfredo. "Intimidad personal, protección de datos personales y geolocalización" *Personal Privacy, Personal Data Protection and Geolocation Apps,* núm. 29, 2015, pp. 47-82. Pág. 48.

[3] BARINAS UBIÑAS, Désirée. "El impacto de las tecnologías de la información y de la comunicación en el derecho a la vida privada". *In Revista electrónica de ciencia penal y criminología* (Issue 15), núm. 15, 2013, pp. 01-60. Pág. 4.

y lo más importante: ¿Somos conscientes de que ya hemos dejado de lado nuestra privacidad por un rato de desconexión de la realidad?

# 2. TRATAMIENTO Y LIMITACIÓN DEL USO DE LOS DATOS DE LOCALIZACIÓN.

## 2.1. Sistemas que permiten la localización.

Por la situación de pandemia que estamos viviendo hemos sido conscientes de que la tecnología cada día forma más parte de nuestro ser, nos envuelve.

Para empezar, tanto el Reglamento General de Protección de Datos como la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, se hacen eco de la posibilidad de que la introducción de tecnologías en las actividades de tratamiento sean un factor que incremente el riesgo para los derechos y libertades de los interesados; riesgo que debe ser evaluado y regulado.

Por lo tanto, en el momento en el que cualquier dato puede ser utilizado por terceros, deberá ser regulado y, como veremos, dependiendo de cada sistema de localización encontramos su regulación dentro de diferentes Leyes o Reglamentos.

Al analizar algunos sistemas de localización nos damos cuenta de que cada vez estamos más limitados en nuestra intimidad; vemos como hasta lo más insignificante, es decir, una búsqueda en Google, conlleva un estudio para un proveedor y así conocer nuestros gustos para que posteriormente se nos invada el correo u otras páginas con anuncios sobre productos que nos puedan interesar o que hayamos hecho alguna búsqueda relacionada días anteriores.

En este apartado iremos analizando concretamente una serie de tecnologías incorporadas en las Administraciones Públicas –en adelante AA.PP.- que conllevan distintos medios de tratamiento de datos personales:

*1.1.1. Cookies.*

Cuando la población empezó a utilizar Internet, se vio la oportunidad de conocer los datos relativos a las personas que visitaban una página web o las veces que se hacía una vista a ésta; si había accedido a ella de una manera directa o a través de otras páginas; si los usuarios se habían registrado en alguna página o, incluso, era posible guardar configuraciones o datos de una sesión.

Por tanto, este sistema de localización permite implementar dichas funcionalidades como, por ejemplo, permitir a los anunciantes conocer qué sitios de Internet visitan los usuarios para ofrecer a éstos productos acordes a sus gustos y, también, a los responsables de los portales, les interesa saber qué páginas han visitado los usuarios para obtener estadísticas y así tomar decisiones para sus anuncios.

Bajo este sistema de localización se enmarcan otros muchos que permiten el seguimiento de los usuarios de forma activa o pasiva; entre éstas se encuentran aquellas que utilizan las características del dispositivo, los identificadores únicos y los hábitos de navegación del usuario. Cada vez que solicitamos una página, una imagen o un contenido a un servidor web, le estamos comunicando, al menos, nuestra dirección IP, con lo que se puede saber nuestra ubicación geográfica, pero también el modelo de navegador que usamos y, en consecuencia, también nuestro sistema operativo, el dispositivo con el que nos conectamos y cómo está de actualizado[4].

El RGPD regula las cookies en su artículo 30[5], reconociendo su capacidad para elaborar e identificar los perfiles de los usuarios. Pero, como normativa específica que regula la utilización de cookies, está el artículo 22.2 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI)[6].

[4] Agencia Española Protección de Datos (España). Tecnologías y Protección de Datos en las AA.PP. [en línea]. [Madrid, 19 de noviembre de 2020]: Notas de prensa. <https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-publica-guia-nuevas-tecnologias-aapp>, login: 'aepd' [Consulta: 31 mar. 2021] p. 10.

[5] "*Las personas físicas pueden ser asociadas a identificadores en línea (…) como direcciones de los protocolos de internet, identificadores de sesión en forma de "cookies" u otros identificadores (…). Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servicios, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas*"

[6] Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico (LISSI) https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758

*1.1.2. Redes sociales.*

Como veremos en el apartado siguiente, donde nos centraremos más concretamente en las Redes sociales y en algunos casos relevantes de éstas, son uno de los canales de información más usados en Internet.

La información puede ser de varios tipos:

- Publicaciones de documentos, textos, fotografías, videos, enlaces, datos de actividad física, etc.

- Comentarios y respuestas a las publicaciones, formando un hilo de diálogo entre publicadores y lectores.

- Perfiles de usuarios, que pueden ser tanto personas físicas como organizaciones. Contienen información personal y de contacto, así como el histórico de sus publicaciones y con qué otros elementos de la red se relacionan (amigos, seguidores, etc.). Las Redes sociales ofrecen diferentes mecanismos de protección de los contenidos de sus usuarios[7].

Actualmente y con la situación pandémica que estamos viviendo, sobre todo los jóvenes, nos hemos involucrado más en las Redes sociales por ser un canal sencillo, accesible e inmediato por el que podemos compartir contenido, socializar con nuestros amigos o familiares, ahora que es más difícil coincidir con ellos, o, incluso, pueden ser un escaparate de productos o servicios con los denominados *influencers*[8].

---

[7] Agencia Española Protección de Datos (España). Tecnologías y Protección de Datos en las AA.PP. [en línea]. [Madrid, 19 de noviembre de 2020]: Notas de prensa. <https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-publica-guia-nuevas-tecnologias-aapp>, login: 'aepd' [Consulta: 31 mar. 2021] p. 16.

[8] El término *influencer* viene definido en la RAE <https://definicion.de/?s=influencer>: Se llama *influencer* a una **personalidad pública que se hizo famosa a través de Internet** y que encuentra en el ámbito digital su principal ámbito de influencia. Se trata de celebridades con **miles o millones de seguidores en las Redes sociales**.

Dentro de todo tipo de Redes sociales existentes en nuestra sociedad, las normas de publicaciones aceptables o etiquetas son las que establezca el proveedor del servicio, que, generalmente, se apoya en una comunidad o estructura participativa[9]. Para la Unión Europea, las Redes sociales encuentran su regulación en el RGPD y en las normativas internas de cada uno de los Estados miembros.

### *1.1.3. Cloud computing o computación en la nube.*

La computación en la nube o *cloud computing* es una forma de usar los servidores en localizaciones remotas de una forma flexible y transparente. En vez de que un usuario obtenga equipos propios, ya sean comprados o alojados en instalaciones concretas, aquél "alquila" equipos virtuales gestionados a través de la Red.

A pesar de que años atrás las herramientas que utilizaba el proveedor eran iguales a las que podía comprar un cliente, en estos momentos existen bases de datos, bibliotecas, lenguajes de programación y componentes software específicos para la nube[10], entre otras cosas.

### *1.1.4. Big Data o tratamiento masivo de datos.*

Al adentrarnos en el concepto del Big Data nos daremos cuenta de que es un sistema por el que se tratan un volumen muy alto de datos.

De acuerdo con la definición dada por ISO[11], cuando hablamos de Big Data o tratamiento masivo de datos, nos referimos a grandes conjuntos de datos caracterizados por su volumen, variedad, velocidad y/o variabilidad, que requieren de una tecnología escalable para su almacenamiento, manipulación, gestión y análisis eficiente.

---

9 Por ejemplo, tenemos las normas de Facebook Community Standards <https://www.facebook.com/communitystandards/>.

10 Amazon Web Services tiene hasta 21 categorías de productos en su nube <https://aws.amazon.com/es/products/>

11 ISO/IEC 20546:2019 Tecnología de la información – Big Data – Resumen y vocabulario.

Como acabamos de ver en su definición, este sistema permite el conocimiento de perfiles de personas y, por ello, precisa de un tratamiento exhaustivo con una legitimación que debe cumplir una serie de requisitos y condiciones; entre ellas, los relativos a las decisiones individuales automatizadas[12] y, en su caso, la realización de una evaluación de impacto para la protección de datos[13] y, si procediese, la consulta previa[14] a la Autoridad de Control competente. Por otra parte, si se han recopilado datos personales, se deben manejar con todas las garantías en cuanto a seguridad[15], derechos[16], transferencias internacionales[17] y otros.

[12] Artículo 22 RGPD – Decisiones individuales automatizadas incluida la elaboración de perfiles. En su apartado primero expresa que "*Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar*".

[13] Artículo 35 RGPD – Evaluación de impacto relativa a la protección de datos. "*Cuando sea probable que un tipo de tratamiento (…) 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 (…).*"

[14] Artículo 36 RGPD – Consulta previa. "*El responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para para mitigarlo.*"

[15] Artículo 32 RGPD – Seguridad del tratamiento. El último apartado regula: "*El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.*"

[16] Artículo 12 RGPD – Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado. En su apartado séptimo regula: "*La información que deberá facilitarse (…) podrá transmitirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto (…).*"

[17] Artículo 44 RGPD – Principio general de las transferencias. "*Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, (…), el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo (…).*"

### *1.1.5. Inteligencia artificial.*

La definición de inteligencia artificial o IA se relaciona con máquinas o sistemas de información que, en el desarrollo de sus funciones, son capaces de aprender de sus propias experiencias y resolver problemas en diferentes situaciones, por lo que parece que "piensan" o muestran una cierta inteligencia[18].

Si nos fijamos en años anteriores, la inteligencia artificial ha sido creada en laboratorios para incorporarse a sistemas cotidianos como, por ejemplo, los buscadores de Internet, la traducción automática, relojes y electrodomésticos inteligentes, aplicaciones móviles, etc.

Lo que más nos interesa dentro de este ámbito son las cuestiones que se plantean en relación con el cumplimiento normativo, la garantía de los derechos de los interesados y la seguridad jurídica de todos los intervinientes.

Si tenemos en cuenta que estos sistemas de Inteligencia Artificial se apoyan en enormes cantidades de datos para aprender y realizar la toma de decisiones, es importante conocer cómo influyen estos datos en este tipo de sistemas y, por consiguiente, garantizar su calidad e integridad, además de evitar que contengan errores o equivocaciones para que estos sistemas no tomen decisiones injustas sobre un tipo determinado de colectivos.

Si analizamos las referencias que hace tanto el RGPD como la LOPDGDD sobre el tratamiento de datos en este sistema, en primer lugar, tenemos que tener presentes las restricciones que establece el artículo 9 del RGPD[19] y el mismo artículo de la LOPDGDD[20], y las condiciones para levantar dicha limitación. Estos artículos regulan unas categorías de datos cuyo tratamiento se prohíbe por cómo puede afectar a los usuarios. Estos datos serían los relativos a un ámbito muy íntimo de los individuos y pueden ser interesantes en el ámbito

---

[18] Agencia Española Protección de Datos (España). Tecnologías y Protección de Datos en las AA.PP. [en línea]. [Madrid, 19 de noviembre de 2020]: Notas de prensa. <https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-publica-guia-nuevas-tecnologias-aapp>, login: 'aepd' [Consulta: 31 mar. 2021] p. 37.

[19] Artículo 9 del RGPD – Tratamiento de categorías especiales de datos personales. "*Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos (…).*"

[20] Artículo 9 del LOPDGDD – Categorías especiales de datos.

mercantil o dentro de las Redes sociales, pero estos datos, al estar dentro de la esfera de la vida privada de cada persona, no pueden ser tratados de cualquier forma. Como vemos, y es en lo que nos vamos a centrar a lo largo de todo este trabajo, existen una serie de límites que tenemos que tener muy claros entre las tecnologías y nuestra intimidad.

## 2.1. Naturaleza de los datos.

### *2.1.1. Datos personales como bien jurídico protegido.*

Los datos de carácter personal, dentro de nuestro ordenamiento jurídico, son un bien protegido y, a la vez, objeto de tráfico jurídico. Por tanto, es necesario una protección al titular de dichos datos por los inconvenientes que puede acarrear el tráfico jurídico de los mismos.

El Derecho reconoce al titular de los datos un poder de disposición y control sobre ellos que se materializa en el derecho a consentir la recogida de los datos, el derecho a oponerse a ella y a su tratamiento; el derecho a conocer la finalidad que se le dará al tratamiento de los datos; el derecho a asegurar una recogida adecuada a la finalidad pretendida; y el derecho a estar informado sobre cómo y dónde se llevará a cabo el almacenamiento y a si accederán terceros a los datos. El poder de disposición se manifiesta a través de la expresión de la voluntad del titular cuando consiente la recogida de los datos y su tratamiento o, en sentido contrario, porque la falta de consentimiento supondrá un tratamiento ilícito de datos que originará responsabilidad[21].

La LOPDGDD, en su Título II relativo a los "Principios de la protección de datos" (artículos 4 a 10) y el RLOPD, en su Título II (artículos 8 a 12), regulan la obtención de los datos personales de los usuarios, el consentimiento que se necesita para el tratamiento de determinados datos, según su categoría y, por supuesto, la información que deben recibir los afectados para proceder a dicho tratamiento; esta información debe ser clara y especificar el uso y la finalidad de los datos recogidos.

[21] BATUECAS CALETRÍO, Alfredo. "Intimidad personal, protección de datos personales y geolocalización", cit., p. 59.

*2.1.2. Tratamiento de los datos de geolocalización: sujetos y momentos en que estos pueden intervenir.*

Centrándonos en nuestro tema, las aplicaciones de geolocalización deben respetar los principios que acabamos de citar. En virtud del artículo 5.1 RGPD, los datos personales que se recaben deben ser tratados de una manera lícita, leal y transparente en relación con el interesado; se deben recoger estos datos de acuerdo con fines determinados, explícitos y legítimos, por consiguiente, los datos deben ser exactos y adecuados para el fin acordado para su tratamiento.

Como iremos estudiando, los dispositivos tienen la opción de conocer nuestra localización y el posicionamiento de nuestro dispositivo, por lo que estamos permanentemente controlados cuando llevamos nuestro terminal o cualquier otro dispositivo con nosotros.

Por ello, nos centraremos en el tratamiento y la información que pueden recabar tanto los fabricantes de dispositivos como las compañías de telefonía, y cómo ejecutan la geolocalización dentro de sus dispositivos. Todo ello es muy importante al estar a la orden día; como todos sabemos, en los tiempos que nos ha tocado vivir con la pandemia, la tecnología ha sido primordial para llevar a cabo nuestra vida en todos los ámbitos.

En cuanto al **fabricante del dispositivo**, existen dos momentos relevantes en cuanto al tratamiento de datos del usuario y, en concreto, a la información que deriva del mismo: primero, cuando se adquiere el dispositivo y, segundo, cada vez que se utiliza la geolocalización.

- En cuanto al momento en que un usuario recibe y/o adquiere el terminal, al tratarse de una compraventa verbal, no se realiza ninguna comunicación de datos personales por parte del usuario. Existe una excepción; es el caso que, durante la venta del dispositivo, el fabricante de éste exija la comunicación de datos personales al usuario con la finalidad de se puedan incorporar a un fichero, esto es, que los datos del afectado tengan un fin comercial.

- El fabricante puede tratar los datos del usuario cada vez que éste utiliza la aplicación de geolocalización. Debemos diferenciar dos situaciones:

    1. Que el fabricante del terminal sólo lo sea del hardware, no del software (quiere decir que el fabricante no es el titular de la aplicación de geolocalización). En

estos casos, aunque el hardware propicia el inicio del tratamiento de los datos personales, ya que ofrece el posicionamiento exacto del terminal, esta transmisión de datos no debe considerarse relevante desde el punto de vista jurídico, al menos en lo que atañe a exigirle obligaciones al fabricante del terminal como responsable de tratamiento de los datos por limitarse su actuación a ser un mero prestador de acceso a servicios de telecomunicaciones o, lo que es lo mismo, un simple colaborador técnico necesario en la transmisión de los datos y cuya labor se circunscribe, no a la de realizar un tratamiento directo de datos, sino a posibilitar tecnológicamente que otro sujeto pueda realizarlo[22].

2. El fabricante, además de que sea titular del hardware, sea autor o titular de la aplicación de geolocalización que se utiliza. Aquí sí que estaría obligado a informar sobre la recogida de datos personales ya que, como titular de la aplicación, es responsable del tratamiento de datos que se va a realizar.

En segundo lugar, el otro sujeto que interviene en esta compraventa es la **compañía telefónica** que facilita la transmisión de los datos. Este sujeto realiza distintos tratamientos de datos, con diferentes finalidades; eso sí, no siempre relacionados con la ejecución de la aplicación de geolocalización, lo que obliga, a su vez, a diferenciar entre varios supuestos.

La compañía telefónica recoge datos principalmente cuando se contrata la línea –en el caso de los teléfonos móviles, se identifica con la adquisición de la tarjeta SIM-. El operador de telefonía recaba estos datos básicamente por dos razones: 1) Los necesita para el correcto mantenimiento de la relación contractual; 2) en ocasiones, con fines comerciales.

Por último, el momento en el que la compañía telefónica participa en el tratamiento de datos del propietario del terminal se origina con la ejecución de la geolocalización y consiste en la transmisión de los datos desde el terminal en el que se encuentra la señal de localización hasta el gestor de la aplicación. La compañía telefónica actúa aquí en calidad de operador de red y como tal recibe el mismo tratamiento que los prestadores de acceso en lo relativo a la aplicación de la legislación de protección de datos. Cuando se ejecuta la aplicación de geolocalización, la compañía telefónica es un mero operador técnico necesario, limitándose

[22] BATUECAS CALETRÍO, Alfredo. "Intimidad personal, protección de datos personales y geolocalización", cit., p. 62.

su intervención a la estricta transmisión de los datos desde el terminal hasta el gestor de la aplicación. Esta remisión de datos que realiza el operador de telefonía es irrelevante desde el punto de vista de la legislación de protección de datos y la compañía telefónica no está obligada a informar sobre ella al usuario del dispositivo[23].

Ejecutada la aplicación de geolocalización, el responsable del tratamiento está obligado a cancelar los datos de localización obtenidos a partir del terminal (artículo 8.6 RLOPD). Los datos no deberán ser conservados de ninguna forma que permita la identificación del interesado durante un periodo superior al necesario para el cual han sido recabados o registrados. Tratar datos más allá del tiempo necesario o del que permita la Ley supone una infracción del artículo 6 LOPDGDD, en tanto este tratamiento no haya sido consentido por el interesado ni se realice con autorización legal.

### 2.3. Consentimiento de los interesados.

#### *2.3.1. Consentimiento mayor de edad.*

En primer lugar, nos tenemos que fijar en el artículo 6 de la LOPDGDD en relación con el artículo 4.11 del RGPD, donde se establece que los datos de carácter personal requieren el consentimiento del afectado, excepto si la ley dispone una regla en contrario. Por otra parte, los artículos 9[24] y 10[25] LOPDGDD regulan categorías especiales de datos de cara a su tratamiento. También se regula el consentimiento para el tratamiento de los datos y el deber de información en el Título II, Capítulo II, del RGPD (artículos 12 a 17).

---

[23] BATUECAS CALETRÍO, Alfredo. "Intimidad personal, protección de datos personales y geolocalización", cit., p. 66.

[24] Artículo 9 LOPDGDD: Categorías especiales de datos. *"(…) el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico*".

[25] Artículo 10 de la LOPDGDD. Tratamiento de datos de naturaleza penal. "*El tratamiento de datos personales relativos a condenas e infracciones penales, así como a procedimientos y medidas cautelares de seguridad conexas (…), solo podrán llevarse a cabo cuando se encuentre amparado en una norma de Derecho de la Unión, en esta ley orgánica o en otras normas de rango legal*".

Cuando tratamos el consentimiento de los interesados, debemos hacernos una pregunta en relación con la geolocalización y con lo relativo al artículo 7 LOPDGDD. ¿Cuándo hablamos del uso de las aplicaciones de geolocalización, este tratamiento no requiere de ningún consentimiento por parte de los interesados? Para dar respuesta a esta cuestión, tenemos que tener en cuenta el artículo 6.1 RGPD[26], donde se regulan una serie de condiciones para que el tratamiento de los datos se considere lícito.

Coincidiendo en este punto con lo ya manifestado por APARICIO SALOM[27], lo que debe inferirse del artículo 6.1 de la LOPDGDD en cuanto a los tratamientos de datos que son esenciales para el mantenimiento o ejecución de un contrato, no es que esos tratamientos constituyan una excepción a la regla general de la exigencia del consentimiento, sino que el consentimiento ya existe desde el momento en que se perfecciona el contrato. Cuando esto ocurra deberá entenderse que el consentimiento al tratamiento de los datos se otorga junto al prestado para la perfección del contrato.

Como viene reflejado en el artículo 6.1 LOPDGDD en relación con el artículo 4.11 RGPD, "*se entiende por consentimiento del afectado toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen*". Como consecuencia de este artículo, todo responsable de los datos que vaya a utilizar de cualquier usuario, previamente deberá asegurarse de que éste manifieste de una manera libre, con una acción afirmativa y específica, que otorga su consentimiento para el tratamiento de sus datos.

*2.3.2. Consentimiento del menor.*

Fijándonos en los menores, se pueden tratar los datos de los mayores de catorce años con su consentimiento, salvo en aquellas situaciones que la ley exija la asistencia de los titulares de la patria potestad o tutela (artículo 7 LOPDGDD).

---

[26] Artículo 6.1 RGPD: "*El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones: a) el interesado dio su consentimiento para el tratamiento de sus datos personales; b) el tratamiento es necesario para la ejecución de un contrato (…); c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento, etc.*".

[27] APARICIO SALOM, Javier, *Estudio sobre la Ley orgánica de protección de datos de carácter personal,* Cizur Menor, Navarra: Aranzadi, 2009, Ed. 3ª. p. 369. Pág. 140-141.

En el caso de los menores de catorce años, se requiere el consentimiento de los padres o tutores –artículo 13.1 RLOPD- y la capacidad que se exige para prestar consentimiento no se debe confundir con aquella que se necesita para la adquisición de un dispositivo o la contratación de la aplicación de geolocalización, que es, en general, la necesaria para obligarse –artículo 1.263 CC-. En el caso de que un menor de catorce años, sin el consentimiento de sus padres, adquiera un dispositivo móvil, este contrato será anulable.

*2.3.3. Solicitud del consentimiento.*

En cuanto a la solicitud de consentimiento, deberá vincular tanto los datos de posicionamiento del terminal con la finalidad que se pretenda con la aplicación, pero, como siempre, delimitando las condiciones especiales si existen (por ejemplo, si los datos van a quedarse almacenados durante cierto tiempo, o si podrán ser cedidos a un tercero).

La prueba de la existencia del consentimiento del titular de los datos recae sobre el responsable del tratamiento, que es el titular de la aplicación de geolocalización (artículo 12.3 RLOPD en relación con el artículo 7 RGPD)[28].

La necesaria prestación de consentimiento del usuario implica que cualquier aplicación de geolocalización deberá estar desactivada por defecto cuando se adquiera el terminal. Por todo ello, es aconsejable que el responsable de la aplicación informe a los usuarios antes de utilizarla por primera vez –así lo indica la Directriz III.2 de la Recomendación nº. R (99) 5 del Comité de Ministros de los Estados miembros sobre la protección de la intimidad en Internet-[29].

Cuando tratamos el tema de los proveedores de servicios de Redes sociales debemos tener en cuenta algunos puntos clave, como son:

[28] BATUECAS CALETRÍO, Alfredo. "Intimidad personal, protección de datos personales y geolocalización", cit., p. 69.

[29] BATUECAS CALETRÍO, Alfredo. "Intimidad personal, protección de datos personales y geolocalización", cit., p. 69.

a) Ser transparentes en relación con sus políticas de privacidad. Cabe precisar que estas reglas deben ser claras, concisas y un fiel reflejo de cómo están utilizando los datos de localización.

b) Adoptar herramientas para que el sujeto concernido pueda en cualquier momento revocar su autorización.

c) Facilitar al titular el acceso a la información recolectada a través de sistemas basados en localización.

d) Implementar mecanismos de "diseño por privacidad" o "*privacy by design*" para evaluar el impacto, valga la redundancia, en la privacidad al momento de desarrollar productos o servicios basados en la localización de sus clientes.

e) Crear conciencia en los cibernautas sobre los riesgos potenciales en el momento en que acceden a páginas web o descargan aplicaciones que carezcan de sistemas de seguridad robustos que permitan, entre otros incidentes, el acceso no autorizado a sus datos personales, o simplemente explicarles cómo pueden desactivar la opción "compartir su ubicación" o impedir que los rastreen[30].

*2.3.4. Tiempo y forma del consentimiento.*

En cuanto al **tiempo** necesario para obtener el consentimiento, deberá obtenerse antes de utilizar la aplicación por primera vez (artículo 16 RLOPD en relación con el artículo 48.2.c) LGT) porque se entiende que en este momento se tratan también por vez primera los datos.

El principio de libertad de **forma** rige en la prestación de consentimiento (artículo 6.1 LOPDGDD en relación con el artículo 4.11 RGPD); también existen una serie de datos

[30] CASTELLANOS MEJÍA, Juan Camilo y MONTEZUMA CHÁVEZ, Luis Alberto, "El uso de sistemas de localización en las plataformas de comunicación en línea o en las Redes sociales", *Revista de Derecho Comunicaciones y Nuevas Tecnologías,* núm. 16, 2016, p.21.

personales cuyo tratamiento queda prohibido, todos ellos regulados en el artículo 9.1 RGPD[31].

Cuando hablamos de consentimiento, lo que se exige es una declaración o acción por parte del afectado que sea claramente afirmativa, consintiendo el tratamiento de los datos personales que le conciernen. Por otra parte, cuando se vayan a utilizar los datos para una pluralidad de finalidades, se deberá contar con dicho consentimiento para cada una de las finalidades de una forma inequívoca (artículo 6.2 LOPDGDD en relación con el artículo 4.11 RGPD). El silencio del interesado que no esté acompañado por ningún acto que pueda interpretarse como una manifestación de voluntad afirmativa al tratamiento de los datos, no podrá considerarse como una prestación de consentimiento (artículo 7 RGPD[32]).

Es por ello y, como conclusión, que son elementos de un código de buena conducta:

a. El compromiso de requerir el consentimiento de los usuarios de manera previa a que sus sistemas de localización identifiquen sus posiciones geográficas. En la práctica, ello se traduce, por ejemplo, en la prohibición de recolectar datos en secreto.

b. La obligación de informar al usuario de las finalidades del tratamiento y, en concreto, en qué momento y por cuánto tiempo esos sistemas estarían autorizados para conocer su ubicación, a saber: por una operación específica o de manera permanente, sin que sea admisible, en consecuencia, cláusulas vagas e imprecisas[33].

El tratamiento de datos de posicionamiento sin el consentimiento de su titular se considera infracción muy grave, como regula el artículo 72.1.c) LOPDGDD[34], y lleva

---

31 Artículo 9.1 RGPD: "*Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos (…)*".

32 Artículo 7.1 RGPD: "*Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales*".

33 CASTELLANOS MEJÍA, Juan Camilo y MONTEZUMA CHÁVEZ, Luis Alberto. "El uso de sistemas de localización en las plataformas de comunicación en línea o en las Redes sociales". *Revista de Derecho Comunicaciones y Nuevas Tecnologías,* núm. 16, 2016, pp. 01-27. Pág. 20.

34 Artículo 72.1.c) LOPDGDD: "*El incumplimiento de los requisitos exigidos por el artículo 7 del Reglamento (UE) 2016/679 para la validez del consentimiento*".

aparejado una sanción de multa de 20.000 euros como máximo (artículo 83.5 c) RGPD). La imposición de la multa no priva al interesado de poder solicitar una indemnización por daños y perjuicios que este tratamiento de los datos le haya causado (artículo 82.1 RGPD en relación con el art. 1101 CC[35]).

Como complemento a la prestación de consentimiento, el titular de los datos debe recibir del responsable del tratamiento, previamente a la recogida de los datos y de modo expreso, preciso e inequívoco, cierta información que se detalla en el artículo 11 LOPDGDD en relación con los artículos 13 y 14 RGPD. En concreto, deberá ser informado sobre:

a) La identidad del responsable del tratamiento y de su representante, en su caso.
b) La finalidad del tratamiento.
c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 RGPD.

Por otra parte, de acuerdo con el artículo 11.3 LOPDGDD, para aquellos datos que no han sido obtenidos del afectado, el responsable del tratamiento dará cumplimiento al deber de información establecido en el artículo 14 RGPD, incluyendo también, además de la anterior, la siguiente información:

a) Las categorías de datos objeto de tratamiento.
b) Las fuentes de las que procedieran los datos.

Para terminar, el propietario del terminal será informado sobre la procedencia de la recogida de los datos y del resto de aspectos contenidos en el artículo 11.1 LOPDGDD durante el proceso de instalación de la aplicación en el dispositivo, o con anterioridad a la primera ejecución de la aplicación.

Es por ello que, para que al propietario del terminal no le quede ninguna duda sobre el alcance que tiene su consentimiento y los datos referentes a su ubicación que serán utilizados por la aplicación de geolocalización cada vez que la ejecute, el titular de la aplicación deberá expresar esta información de una manera precisa, expresa e inequívoca. La ausencia de esta información o un mero aviso, se considerará incumplimiento del deber de información.

---

[35] Artículo 1101 CC: "*Quedan sujetos a la indemnización de los daños y perjuicios causados los que en el cumplimiento de sus obligaciones incurrieren en dolo, negligencia o morosidad, y los que de cualquier modo contravinieren al tenor de aquéllas*".

## 3. GEOLOCALIZACIÓN: REDES SOCIALES.

En la época que vivimos existe un mundo virtual que nos proporciona una gran variedad de información, donde podemos acceder a todo lo que necesitamos con un simple "clic". Llega un momento en el que no podemos diferenciar con claridad lo que es el mundo físico de lo que es el mundo virtual, ya que éste último nos proporciona todo lo que queremos en tiempo record. El problema es que, cuando nos involucramos en el mundo de Internet, dejamos a nuestro paso cierta información sobre nosotros; simplemente con una búsqueda de un lugar donde queramos ir, en Internet ya queda plasmado uno de nuestros gustos y la ciudad que tenemos pensado visitar.

Por lo tanto, Internet es una gran base de datos tanto para buscar información como para que, a través de las páginas que hayamos visitado, se nos pueda realizar una lista de objetos, sitios, etc., que nos puedan interesar, solo y exclusivamente con haber hecho "clic" en una página web.

La localización se define como "*un concepto que hace referencia a la situación que ocupa un objeto en el espacio y que se mide en coordenadas de latitud (x), longitud (y) y altura (z)*"[36].

Debemos entender que, a través de los sistemas de localización, se permite identificar la ubicación exacta de un individuo a través de Internet. Por lo que hemos estudiado en el primer epígrafe, el método más utilizado para ello es la dirección IP del usuario. Este método funciona de la siguiente manera:

a. Cuando el usuario escriba una URL (localizador de recursos uniforme) en su navegador como, por ejemplo, Google, Mozilla o Big, o hace clic en un hipervínculo, dicha solicitud de acceso se envía al servidor donde opera el sitio Web.

b. Cuando ese servidor recibe la solicitud de acceso, este envía una solicitud de ubicación de la dirección IP del usuario al proveedor de servicios de geolocalización.

c. El proveedor de servicios de geolocalización, con base en la información de las direcciones IP en uso recopiladas por él en su base de datos, le suministra al servidor del sitio Web una pista de dónde se encuentra la ubicación del usuario final.

[36] CASTELLANOS MEJÍA, Juan Camilo y MONTEZUMA CHÁVEZ, Luis Alberto. "El uso de sistemas de localización en las plataformas de comunicación en línea o en las Redes sociales", cit., p.13.

d. Con esa información, el servidor Web proporciona el acceso al usuario final[37].

### 3.1. Redes sociales.

En el mundo cibernético no existe una definición oficial de las Redes sociales, algunos autores las han definido como "*servicios prestados a través del Internet que permiten a los usuarios generar un perfil público, en el que plasmar datos personales e información de uno mismo disponiendo de herramientas que permiten interactuar con el resto de usuarios afines o no al perfil publicado, ya sea publicando imágenes, vídeos o compartiendo otro tipo de información*"[38].

En la actualidad, todo individuo conoce o utiliza alguna Red social, ya sea para comprar vía Internet o para relacionarnos con nuestros amigos o familiares que estén lejos de nosotros. A través de las Redes sociales, los usuarios hablan con sus amigos, publican fotos de los lugares que visitan, o, incluso, en una Red social como Google se pueden identificar los sitios visitados por el usuario.

Por lo tanto, en este mundo virtual denominado Internet, los usuarios pueden crearse una sociedad, relacionándose con otros individuos y compartiendo intereses comunes; aquí no existe un límite físico que separe a las personas, sino que todos pueden comunicarse con todos.

Es por esta razón que parte de su modelo de negocio es identificar la ubicación del usuario o personas en común con el fin de sugerir grupos de contactos precisos con base en intereses comunes, actividades y productos o servicios dentro de su localización[39].

---

[37] CASTELLANOS MEJÍA, Juan Camilo y MONTEZUMA CHÁVEZ, Luis Alberto. "El uso de sistemas de localización en las plataformas de comunicación en línea o en las Redes sociales", cit., p.14.

[38] BARINAS UBIÑAS, Désirée. El impacto de las tecnologías de la información y de la comunicación en el derecho a la vida privada, cit., pp. 30-31.

[39] CASTELLANOS MEJÍA, Juan Camilo y MONTEZUMA CHÁVEZ, Luis Alberto. "El uso de sistemas de localización en las plataformas de comunicación en línea o en las Redes sociales", cit., p.16.

Podemos diferenciar dos tipos de Redes:

a) Aquellas cuya función se estructura dentro de una arquitectura cliente-servidor. La información se encuentra centralizada en un servidor y es allí donde funciona la plataforma.

b) Aquéllas que funcionan a través de un peer-to-peer. La información se encuentra distribuida entre los diferentes usuarios de la red, es decir, no se encuentra centralizada[40].

La gran mayoría de plataformas se encuentran centralizadas como, por ejemplo, Facebook o Twitter; Redes sociales que hoy en día son bien conocidas. En ellas, todo el contenido se encuentra almacenado en los propios servidores de cada aplicación y/o compañía. Los proveedores de estas compañías incorporaron una nueva herramienta, la ubicación de sus usuarios, que, a la larga, puede servir para identificar los gustos de cada individuo y así exponerle ciertas páginas o ciertos productos que puedan interesarle.

Existen Redes sociales conocidas por su nombre en inglés como "*Location Based Social Networks*" (LBSN), que permiten compartir la ubicación de sus usuarios utilizando un sistema cuya base es la localización, ya sea a través de equipos móviles o de ordenadores de escritorio. En estos portales encontramos dos maneras de compartir la posición de los individuos:

1. *Geotagging*: Los vídeos, fotos, blog post o tweets son convertidos en información geográfica y el usuario identifica dónde se encuentra ubicado en ese instante.

2. *Geosocial networking*. Cuando los usuarios comparten en su perfil su ubicación actual; incentiva a compartir la información por medio de juegos o aplicaciones gratuitas[41].

[40] CASTELLANOS MEJÍA, Juan Camilo y MONTEZUMA CHÁVEZ, Luis Alberto. "El uso de sistemas de localización en las plataformas de comunicación en línea o en las Redes sociales", cit., p.16.

[41] CASTELLANOS MEJÍA, Juan Camilo y MONTEZUMA CHÁVEZ, Luis Alberto. "El uso de sistemas de localización en las plataformas de comunicación en línea o en las Redes sociales", cit., pp.17-18.

Por ejemplo, en Facebook se permite conocer la ciudad exacta de cada usuario y, en relación con esta ubicación, se actualiza la configuración y la localización de determinados restaurantes o tiendas. Lo mismo ocurre con Twitter, donde los usuarios pueden compartir información de su localización en sus actualizaciones, todo ello dentro del marco de la configuración de dicha Red social.

Aparte, la propia estructura de Internet hace posible que la información sea interceptada en cualquiera de las etapas de la trayectoria por la que pasa un paquete de información, ya que el mismo circula por diversos sitios hasta llegar a su destino final[42]. Todo ello plantea serios problemas en cuanto a nuestra privacidad dentro de las Redes sociales, ya que habría que determinar quién es el responsable de salvaguardar toda la información que se encuentre dentro de esta estructura.

Se puede concluir que el modelo de negocios de este tipo de servicios funciona en el "intercambio o consumo de información personal", dado que las Redes sociales ofrecen al usuario servicios aparentemente gratuitos pero cuya contraprestación no es otra que acceder a sus datos personales y obtener información directamente requerida al usuario con finalidades como la elaboración de perfiles de consumo o personalidad, o remitirle determinada información o publicidad[43].

Como acabamos de ver, todos los que utilizamos una Red social, ya sea Facebook o Instagram, en donde creemos en un primer momento que la podemos usar de forma gratuita ya que no nos piden ninguna contraprestación por darnos de alta en ellas, estamos pagando con algo más caro que el dinero, con nuestra intimidad, nuestros datos, nuestros gustos, etc. Todo ello queda expuesto a una gran compañía, que los utiliza y manipula para su propio beneficio. Pueden conocernos, saber lo más íntimo de cada usuario, tener en su poder todas las fotos que "subamos"; fotos que, una vez subidas en Internet, perdemos el poder sobre ellas, dejan de estar en "nuestra propiedad" para poder estar en manos de cualquier persona.

[42] BARINAS UBIÑAS, Désirée. El impacto de las tecnologías de la información y de la comunicación en el derecho a la vida privada, cit., p.21.

[43] CASTELLANOS MEJÍA, Juan Camilo y MONTEZUMA CHÁVEZ, Luis Alberto. "El uso de sistemas de localización en las plataformas de comunicación en línea o en las Redes sociales", cit., p.17.

De este modo se pasa a ser tanto sujeto de los datos posteados como generador de la información publicada, muchas veces sin tener una verdadera comprensión de sus implicaciones, dentro de una memoria digital que todo lo recuerda, lo guarda y lo pone a disposición[44].

### 3.2. Tratamiento y transparencia de los datos personales.

#### *3.2.1. Tratamiento de los datos personales.*

Cuando estudiamos el concepto de "*tratamiento de datos personales*" lo debemos abordar desde la perspectiva de que se trata de procedimientos técnicos, todos ellos con origen en comunicaciones, consultas o transferencias, que permiten recabar grabaciones, conservar toda la información allí recopilada, elaborar, modificar, utilizar, etc.; todo ello recogido en el artículo 5.1.t) RLOPD[45].

La LOPDGDD, en su artículo 1, refleja su objetivo principal, que es el de adaptar el ordenamiento jurídico español al RGPD y garantizar los derechos digitales de los ciudadanos.

Se puede entender que todo dato personal está bajo el amparo de la LOPDGDD desde el momento en el que se somete a operaciones de tratamiento. Toda actividad del responsable del tratamiento está ordenada por la norma y, además, se canaliza para proteger el ejercicio del derecho subjetivo relativo a la información personal.

Pueden tratarse como datos personales aspectos tan diversos como la imagen (aspecto físico, datos biométricos), la información perteneciente a la esfera profesional (titulación, adscripción a colegios profesionales) o económica (nivel de solvencia o de riesgo, condición de cliente minorista), las costumbres (recorridos habituales, hábitos de compra, visitas a un lugar), los datos referentes a la salud (enfermedades, información genética, días en que se acudió a un hospital) y los datos de contacto (dirección de correo electrónico, números

[44] BARINAS UBIÑAS, Désirée. El impacto de las tecnologías de la información y de la comunicación en el derecho a la vida privada, cit., p.30.

[45] Artículo 5.1.t) RLOPD: "*Tratamiento de datos: cualquier operación o procedimiento técnico (…) que permita la recogida, grabación, conservación, elaboración, modificación (…), así como las cesiones de datos que resulten de comunicación, consultas, interconexiones y transferencias*".

telefónicos) y los identificadores (número del Documento Nacional de Identidad o un número PIN)[46].

A continuación, pasaremos a estudiar determinados perfiles de los sujetos y su utilización para la comercialización.

### *3.2.2. Perfiles de los sujetos.*

#### *3.2.2.1. Perfiles: identificación cualitativa del individuo[47].*

Todos los tratamientos de datos de los usuarios permiten crear perfiles con una información exacta y pormenorizada asociada a un individuo en una categoría diferente. Es por ello que, cuanto analizamos el concepto de "*dato personal*", vemos como comprende tanto la información única del usuario como el perfil de la personalidad que resulte del cruce de datos.

El "*perfil*" define un aspecto de la personalidad y se diferencia del dato concreto en que es el producto del tratamiento y ofrece una identificación cualitativa, más rica y útil que la identificación que proporciona el nombre. El perfil representa el paso intermedio entre el registro de los datos personales y su aplicación a decisiones individualizadas. Asimismo permite anticipar las conductas y tomar decisiones preventivas[48].

Como he apuntado arriba, el perfil es el resultado del tratamiento que, partiendo del registro de los datos, proporciona un producto distinto. Constituye una información mediata porque no la ha proporcionado directamente el afectado; parcial porque ofrece una visión incompleta sobre el individuo; nueva porque resulta de un proceso organizado por el responsable del tratamiento que el afectado no podía proporcionar; y descontextualizada

---

[46] LLÁCER MATACÁS, María Rosa. *La autorización al tratamiento de información personal en la contratación de bienes y servicios*. España: Dykinson, 2012., pp. 188. Pág. 32.

[47] LLÁCER MATACÁS, María Rosa. *La autorización al tratamiento de información personal en la contratación de bienes y servicios*, cit., p.33.

[48] LLÁCER MATACÁS, María Rosa. *La autorización al tratamiento de información personal en la contratación de bienes y servicios*, cit., p.34.

porque puede aplicarse a fines sin relación con el hecho que motivó la revelación de los datos originarios[49].

*3.2.2.2. El uso de perfiles dentro del ámbito comercial.*

Como ya hemos ido analizando poco a poco durante el trabajo, el perfil de todo usuario sirve como instrumento de decisión comercial que detecta a los mejores perfiles de usuarios para sus ofertas o, por el contrario, a los clientes menos deseados.

Desde esta idea van surgiendo las llamadas "*políticas de privacidad*" que las empresas definen a fin de asegurar el mercado (pero cuyo contenido no es regulado en todos los países) e "informar" a sus usuarios a fin de obtenerse el consentimiento informado de los mismos en el tratamiento de sus datos personales. Si bien, no dejan de ser acuerdos de adhesión en los que las opciones se reducen a aceptarlos y tener acceso a un determinado bien o servicio, o no aceptarlos y autoexcluirse del mismo[50].

Como es sabido, todos nosotros, a través de Internet, estamos siendo vigilados y tenemos que tener conciencia de que la información que dejamos a nuestro paso por la Web es utilizada para que nos lleguen solicitudes, ofertas y anuncios que nunca pedimos. Aquí surge la problemática denominada "*opt in*[51]" y "*opt out*[52]", si bien la mayoría de los defensores de la privacidad entiende que el consentimiento previo para la recepción de publicidad deber ser necesario.

Es por ello que las comunicaciones comerciales que no son solicitadas por el internauta, presentan un doble atentando a la privacidad: por un lado, consecuencia de la utilización de los datos de carácter personal como, por ejemplo, el correo electrónico de un sujeto, para un

---

[49] LLÁCER MATACÁS, María Rosa. *La autorización al tratamiento de información personal en la contratación de bienes y servicios*, cit., p.35.

[50] BARINAS UBIÑAS, Désirée, El impacto de las tecnologías de la información y de la comunicación en el derecho a la vida privada, cit., p.46.

51 "*Opt-in*": es cuando un usuario se suscribe y acepta recibir informaciones por email. https://www.rdstation.com/es/blog/opt-in/amp

[52] "*Opt-out*": es el link para darse de baja, presente en los emails enviados. https://www.rdstation.com/es/blog/opt-in/amp

uso no autorizado por el titular; y, por otro, la intromisión que pueda generar al sujeto y la perturbación de su "paz" el recibir información no deseada de una manera continuada y excesiva.

Existe una problemática en relación con la regulación existente en otros países donde es usual aceptar el tratamiento no consentido de datos personales "*necesarios para el servicio*", que implica la recolección y manipulación de información que no es especificada al usuario, y que también puede ser transferida a terceros que no han sido identificados y, por tanto, de los que el usuario desconoce de su existencia.

En España, encontramos el concepto *opt-in* derivado del Reglamento General de Protección de Datos, que establece que este permiso debe ser de una manera activa, es decir, dentro de un formulario web, se debe incluir una casilla con un mensaje como "*Desea recibir mensajes de marketing de una marca X*" y el usuario, si lo quiere, deberá hacer clic en esta casilla de una forma activa. El concepto *opt-out* dejó de ser utilizado cuando se aplicó el citado Reglamento por creer que no se ajustaba a la nueva normativa.

En el momento que se invade la tranquilidad individual del destinatario de la comunicación comercial a través de diferentes canales de comunicación, ya sea en su domicilio, a través de llamadas telefónicas, correo electrónico, etc., se debe analizar si el tratamiento es ilícito, es decir, no consentido –artículo 6.1 LOPDGDD-, en cuyo caso el afectado podrá ejercer su derecho de oposición (artículo 18 LOPDGDD).

Por el contrario, si el tratamiento es legítimo porque el individuo consintió o porque los datos provienen de fuentes accesibles al público, el afectado podrá revocar el consentimiento (artículo 17.1 RLOPD) o bien hacer cesar el tratamiento ejerciendo el derecho de oposición en los términos del artículo 34.a) y b) RLOPD.

La creación de perfiles dentro del mercado puede acarrear una discriminación a las personas. Los datos obtenidos pueden utilizarse para diferentes fines, por ejemplo, el diseño de estrategias comerciales, la adopción de decisiones individuales automatizadas que llevan una clasificación de los usuarios en Internet, que pueden acarrear una lista de clientes "no rentables".

El acto de discriminación representa un trato desfavorable aplicado a situaciones comparables y no amparado en un fin legítimo. Puede darse de forma directa, cuando se trata a una persona de manera menos favorable que a otra en una situación comparable, o indirecta, cuando una decisión aparentemente neutra coloca a un grupo de personas en

desventaja con respecto a personas pertenecientes a otro, salvo que pueda justificarse objetivamente en una finalidad legítima y que los medios sean necesarios y adecuados[53].

Esa lista de clientes "no rentables" puede acarrear un peor trato o servicio dentro de un comercio por el simple hecho de que se les haya clasificado dentro del grupo de personas que pueden no ser suficientemente rentables. Y esto puede ser un peligro tanto en aquellas empresas que ofertan en línea, o en tiendas "físicas", ante el mercado de información que contiene Internet de las cosas y personas.

Para terminar, el artículo 36.1 RLOPD señala que "*los interesados tienen derecho a no verse sometidos a una decisión con efectos jurídicos sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, tales como su rendimiento laboral, crédito, fiabilidad o conducta*"[54]. Por su parte, la LOPDGDD, en su artículo 11.2, en lo que a información se refiere, añade que "*el afectado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar*".

#### *3.2.2.3. La concurrencia de intereses sobre los perfiles: el interés inherente del afectado y el interés legítimo del responsable del tratamiento[55]*

El proveedor reúne dos intereses:

1. <u>El inherente al contrato</u>, que consiste en obtener un lucro derivado de la prestación del bien o servicio, al que eventualmente se añade el interés en obtener los datos para

[53] LLÁCER MATACÁS, María Rosa. *La autorización al tratamiento de información personal en la contratación de bienes y servicios*, cit., p.39.

[54] Así también el artículo 22 RGPD, que reconoce el derecho que tiene todo interesado de no ser objeto de este tipo de decisiones, estableciendo también una serie de excepciones en caso de que la decisión sea: "*a) necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento; b) está autorizada por el Derecho de la Unión (…); c) se basa en el consentimiento explícito del interesado*".

[55] LLÁCER MATACÁS, María Rosa. *La autorización al tratamiento de información personal en la contratación de bienes y servicios*, cit., p.45.

fines propios, ajenos al contrato. La ejecución contractual es un interés legítimo del responsable (artículos 10.3 b) y 10.4 a) RLOPD) compartido con el afectado.

2. El uso de información para fines ajenos al contrato interesa siempre al responsable y, eventualmente, al afectado, por ejemplo para estar informado sobre temas de su interés[56].

Por lo tanto, para el primero de los intereses, teniendo en cuenta el artículo 6.1.b) RGPD, es lícito el tratamiento de datos que resulta "*necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales*". En cambio, para el segundo, el proveedor-responsable deberá solicitar el consentimiento del afectado de conformidad con lo regulado en el artículo 12.2 RLOPD[57].

El artículo 46 RLOPD refleja dos formas de rentabilizar los datos:

1. El responsable del tratamiento lleva a cabo, en su propio nombre, la actividad publicitaria de sus productos o servicios entre sus clientes (apartado primero); aquí también debemos tener en cuenta el artículo 6.1 LOPDGDD sobre el consentimiento del interesado, ya que sin éste no se podrá llevar a cabo de una manera lícita dicha actividad publicitaria.

2. La celebración de un contrato de campaña publicitaria con una determinada empresa (apartado segundo). En este caso, el tratamiento se realiza sobre una base de datos de la empresa con la que se contrata y este artículo, como veremos a continuación, nos proporciona los criterios para determinar si el responsable del tratamiento es el arrendatario del servicio, o con quien encarga la campaña la propia empresa.

---

[56] LLÁCER MATACÁS, María Rosa. *La autorización al tratamiento de información personal en la contratación de bienes y servicios*, cit., p.46.

[57] Artículo 12.2 RLOPD: "*Cuando se solicite el consentimiento del afectado para la cesión de sus datos, éste deberá ser informado de forma que conozca inequívocamente la finalidad a la que se destinarán los datos respecto de cuya comunicación se solicita el consentimiento y el tipo de actividad desarrollada por el cesionario (…)*".

Todo ello depende de quién proporciona los criterios identificativos o perfiles a utilizar (artículo 46.4 RLOPD[58]):

- Si los fija la entidad que contrata la campaña: ésta será la responsable del tratamiento de los datos que se lleguen a manejar.

- Si los fija la entidad o entidades contratadas: ésta responderá al ser la única responsable del tratamiento (artículo 46.2.b) RLOPD).

- Si intervienen ambas: serán ambas responsables del tratamiento (artículo 46.2.c) RLOPD).

Por lo tanto, este artículo regula los dos colectivos empresariales con intereses en los datos personales de la clientela: tanto los proveedores de bienes y servicios como las empresas que ofrecen servicios publicitarios.

Para terminar, decir que existe una tercera forma de rentabilizar la información personal: la cesión o comunicación a terceros, presupuesta la autorización del afectado (artículo 10.1 RLOPD[59]).

### *3.2.3. Transparencia.*

Los datos personales dentro de la llamada "Sociedad de la Información" en la que nos encontramos en la actualidad, han sido objeto de una mercantilización en tanto que representa una "riqueza" para aquellos que los posean. Todos nuestros datos y, con ellos, la información que se pueda obtener, hoy en día tienen un precio, por lo que podríamos defender que ya no estamos hablando de un derecho sobre los datos personales de cada usuario, sino que sería tratado como un derecho de propiedad, una especie de híbrido, que aproxima su protección a la de los bienes intelectuales.

---

58 Artículo 46.4 RLOPD: *"(…), se consideran parámetros identificativos de los destinatarios las variables utilizadas para identificar el público objetivo o destinatario de una campaña o promoción comercial de productos o servicios que permitan acotar los destinatarios individuales de la misma*".

59 Artículo 10.1 RLOPD: "*Los datos de carácter personal únicamente podrán ser objeto de tratamiento o cesión si el interesado hubiera prestado previamente su consentimiento para ello*".

Todo esto genera una fracción entre la clásica visión de la vida privada como un derecho fundamental y personal, y la demanda de la cibereconomía donde el flujo y manipulación de los datos es uno de sus elementos principales y donde la tradicional idea de la *privacy* se contempla como un freno al desarrollo del comercio electrónico y de los negocios "en línea". Sin embargo, esta visión económica de la naturaleza de los datos personales, en cuanto al contenido de su protección se refiere, no deja de suscitar problemas que rebasan el aspecto jurídico al recontextualizar la concepción misma que coloca al ser humano como un fin y no como un medio en la sociedad de consumo[60].

Por tanto, uno de los principales problemas que existe dentro de la protección del derecho a la vida privada, es el modo en que lo ejercemos los titulares, que, muchas veces, exponemos de forma aleatoria y muy alegremente nuestros datos personales, sin ser conscientes de lo que acarrea esta exposición.

Como defiende BARINAS UBIÑAS[61], *Internet conllevó el nacimiento de una "nueva" economía en la que se intensifica la competencia sin fronteras frente a ofertantes que ni siquiera necesitan existir "físicamente" y en la que el consumidor, se dice, es el "rey". Sin embargo, no es menos cierto que con ella viene una infraestructura de vigilancia y trazabilidad, y el desarrollo de un modelo de negocio en el que no siempre se paga con dinero, sino con datos; todo ello para brindar un servicio mejor ya que "el cliente así lo quiere".*

#### *3.2.3.1. Transparencia en el ámbito estatal.*

Tenemos que tener en cuenta que el empeoramiento económico ha fomentado que se desarrolle una tecnología invasiva; pero también hay es cierto que los gobiernos han contribuido para conseguir el control del ciudadano con este tipo de tecnología, justificando dicha operación con la lucha contra el crimen organizado y el terrorismo, llegando al mayor extremo a partir del día 11 de septiembre de 2001.

El Estado y los ciudadanos interactuamos con las TIC,s desde dos perspectivas:

---

[60] BARINAS UBIÑAS, Désiré. El impacto de las tecnologías de la información y de la comunicación en el derecho a la vida privada, cit., p.38.

[61] BARINAS UBIÑAS, Désirée. El impacto de las tecnologías de la información y de la comunicación en el derecho a la vida privada, cit., p.39.

- Como usuarios de servicios públicos en el llamado "e-goverment" o administración electrónica.
- Como entes sujetos a la vigilancia estatal[62].

#### *3.2.3.2. "E-goverment" o administración electrónica.*

El Estado es quien posee una mayor cantidad de datos personales, es quien gestiona dentro de sus funciones públicas informaciones que va desde el nacimiento hasta la muerte de cada ciudadano, incluso nuestro nombre, estado civil, etc., y por supuesto, aquellos datos generados en la administración de servicios públicos.

La institución estatal ha integrado las nuevas tecnologías garantizando la transferencia y la eficacia de las mismas**.** Ello lleva a que la digitalización de la información y su integración en la red acarreen problemas, sobre todo cuando hablamos de interconexión de bases de datos estatales, transferencias interadministrativas y del incremento de la publicidad de los datos personales (con la cantidad de información que éstos recolectan).

En todos los Estados surge el problema de equilibrar la eficacia de la Administración Pública y la protección de los datos personales, con tratamientos que, en la mayoría de los casos, pueden permanecer ocultos al ciudadano por justificarse en una "cooperación interinstitucional". Todos los datos gestionados por la Administración Pública parecerían formar parte del "aparato estatal", lo que puede llevar al abuso del acceso a la información[63].

En la actualidad, el Estado se enfrenta al reto de garantizar la utilización de los datos personales con un fin legítimo y gestionarlos correctamente frente a las exigencias de acceso a la información pública.

Los derechos fundamentales funcionan como límites al poder estatal para poder garantizar el respeto de unas prerrogativas mínimas para el desarrollo de una vida digna. Pero estos últimos años hemos sabido que el concepto de "seguridad" sobrepasa todos aquellos

[62] BARINAS UBIÑAS, Désirée. El impacto de las tecnologías de la información y de la comunicación en el derecho a la vida privada, cit., p.51.

[63] BARINAS UBIÑAS, Désirée. El impacto de las tecnologías de la información y de la comunicación en el derecho a la vida privada, cit., p.53.

valores principales del Estado, que éste parece olvidar que existen unos límites, al menos en lo relativo a las ideas de libertad y dignidad humana.

Existe una excepción justificada sobre la información de la vida privada de las personas que han sido condenadas por delitos graves; ya que, antes de llegar a esta decisión firme al respecto, ha sido necesario recopilar información suficiente y veraz para fundamentarla, es decir, recopilar todo lo necesario de sus actividades financieras o las intervenciones telefónicas de dichos condenados. Y, en este caso, se ha dejado de lado su intimidad porque, ante todo, era necesario recopilar las pruebas suficientes para tomar una decisión.

Ponemos como ejemplo la STS 141/2020, Sala Segunda, de lo Penal, de 13 de mayo de 2020, Rec. 2749/2018 (RJ 2020\1150), en la que se absuelve a un acusado de tráfico de drogas por haber colocado un dispositivo GPS en su vehículo. Como consecuencia de la vulneración de su derecho a la intimidad, todas aquellas pruebas que fueron aportadas durante el juicio debieron ser consideradas nulas como también las diligencias realizadas por los agentes durante el juicio -incautación de drogas en el vehículo intervenido-. Se concluyó que "*existió una eficacia invasora de los dispositivos de rastreo y geolocalización*".

Ya hemos visto lo que supone la vigilancia estatal, pero también existe la privada, entre particulares; en este caso, tenemos la Sentencia de la Audiencia Provincial de Cádiz, Sección 8ª, Sentencia 126/2019, de 30 Julio de 2019, Rec. 193/2019 (JUR 2019\341579), que considera una intromisión ilegítima la instalación por el detective demandado de un dispositivo de geolocalización en el vehículo del actor para demostrar la existencia de una relación sentimental con la ex esposa de quien contrató al detective[64].

Es por esto necesaria una protección de los "*datos personales*", cuya recolección, conservación, manipulación y transmisión de forma indebida o ilícita puede atentar contra el derecho a la vida privada de cada sujeto.

[64] Esta Sentencia concluye que "*la finalidad de acreditar que la ex esposa podía tener una ocupación laboral y, a la vez, una relación sentimental no justifica el seguimiento que se la estaba realizando; porque quien controla el dispositivo conoce con total exactitud los desplazamientos que estaba realizando la mujer, y ello impide que el sujeto pueda reservar un ámbito de su vida privada*".

### 3.3. Derechos del interesado y consecuencias del uso de las Redes sociales.

*3.3.1. Derechos del interesado en relación con la transparencia de sus datos.*

Es una realidad que la participación en las Redes sociales nos da innumerables ventajas, pero, como contraparte, también implica una serie de riesgos para los usuarios, siendo mayores en los menores de edad desde el momento en el que se registran en la Red e interactúan con ciertas personas que, en muchas ocasiones, no saben quién se esconde detrás de ese perfil. Otro riesgo es el de la localización; herramienta que se utiliza en todas las Redes sociales y que nos puede perjudicar a nuestra intimidad como usuario. Las Redes se basan en sistemas de localización con el fin de enriquecer la experiencia del usuario. También lo consiguen cuando son los usuarios los que comparten su ubicación a los contactos que tengan dentro de la misma. Pero estas dos situaciones se deberán basar en la autorización del usuario para que funcionen los sistemas basados en la localización. Es por ello que toda Red social tiene la obligación de implantar en sus portales la decisión de que sus servicios incorporan la ubicación de los usuarios.

La gestión de los datos personales expuestos en las Redes sociales y su protección es en gran medida responsabilidad de los prestadores de servicios que ofrecen la interrelación. Inicialmente definida en declaraciones dadas a conocer a los usuarios antes de integrarles en ellas, no siempre queda claro, sin embargo, quién es el responsable del tratamiento de los datos que se vayan ofreciendo. Los usuarios deben expresar su aceptación a dicho tratamiento y lo más que proclaman los prestadores de servicios, en la mayoría de los casos, es su "respeto por la privacidad", conscientes, eso sí, de que el principal elemento para ganar a los navegantes *on line* es el nivel de confianza que inspiren[65].

Las siguientes herramientas podrían ser modificadas en las Redes sociales por los usuarios que no quieran que se conozca la localización de su perfil, o lo que publican en ella:

1. Faceebook: la opción de localizar a los usuarios y sus acciones en el muro.

2. Twitter: los tweets que lanza tienen la opción de seleccionar la localización.

[65] BARINAS UBIÑAS, Désirée. El impacto de las tecnologías de la información y de la comunicación en el derecho a la vida privada, cit., p.33.

3. Linkedln: la opción "Ubicaciones principales en tu red" en el apartado de estadísticas, localización y Redes sociales.

4. Foursquare: opción de los usuarios de hacer pública su localización.

5. Instagram: posibilidad de identificar la ubicación donde fue tomada la foto en función de las personas, los lugares y las etiquetas[66].

Las autoridades de protección de datos a nivel mundial y algunos académicos han tomado conciencia sobre el tratamiento que se está dando a los datos personales en las Redes sociales, más aún cuando se recolectan datos, se tratan y comparten por algunos servicios web, como por ejemplo Messenger de Facebook, sin que exista una previa autorización y, en algunos casos, sin que muchos usuarios conozcan la finalidad principal del tratamiento o los derechos que pueden ejercer frente a estos servicios.

Al mismo tiempo se han identificado tres riesgos a la privacidad de los sistemas de localización, que deberían ser tenidos en cuenta tanto por las Redes sociales como por los usuarios:

a) Riesgo de privacidad de localización, que quiere decir que cualquier persona puede conocer dónde se encuentra determinada persona en cierto momento.

b) Riesgo de ausencia de privacidad, que implica poder conocer que una persona no se encuentra en determinado sitio, por ejemplo, en el trabajo.

c) Riesgo de co-localización de privacidad, por el cual una persona se puede localizar por medio de la identificación de otros usuarios con algún tipo de vínculo dentro del portal[67].

---

[66] CASTELLANOS MEJÍA, Juan Camilo y MONTEZUMA CHÁVEZ, Luis Alberto. "El uso de sistemas de localización en las plataformas de comunicación en línea o en las Redes sociales", cit., p.19.

[67] CASTELLANOS MEJÍA, Juan Camilo y MONTEZUMA CHÁVEZ, Luis Alberto. "El uso de sistemas de localización en las plataformas de comunicación en línea o en las Redes sociales", cit., p.18.

Consecuencia de que los datos de posicionamiento del terminal de un usuario sean tratados por la aplicación de geolocalización, el titular de los mismos podrá ejercitar los derechos de acceso, rectificación, oposición o cancelación que se reconocen en los artículos 13 a 18 LOPDGDD en relación con los artículos 27 a 36 RLOPD.

Por el derecho de acceso[68] (artículo 13 LOPDGDD en relación con los artículos 27 a 30 RLOPD), el titular de los datos podrá solicitar y obtener información relativa a qué datos personales suyos han sido objeto de tratamiento, a cómo se han obtenido y a todo lo referente a las comunicaciones que se quieren hacer con ellos[69].

El titular de la aplicación de geolocalización está obligado a resolver sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud (artículo 29 RLOPD). Transcurrido el plazo sin que de forma expresa el titular de la aplicación de geolocalización responda a la petición de acceso, el interesado podrá reclamar ante la AEPD y ésta derivarlo al delegado de protección de datos, según se establece en el artículo 37.2 LOPGDDD. El titular de la aplicación de geolocalización podrá denegar el acceso a los datos de carácter personal cuando el derecho ya se haya ejercitado en los doce meses anteriores a la solicitud, salvo que se acredite un interés legítimo al efecto (artículo 29.3 RLOPD)[70].

Cuando un interesado ejerce su derecho de rectificación y cancelación (artículos 14 y 15 LOPDGDD relacionado con los artículos 31 a 33 RLOPD), solicita al titular de la aplicación de geolocalización la rectificación o supresión de los datos que se han estado tratando. En el caso concreto del derecho de rectificación, el sujeto lo que quiere es que se modifiquen aquellos datos sobre los que previamente haya dado su consentimiento para el tratamiento, y *resulten ser inexactos o incompletos*, por lo que todas las solicitudes de rectificación deberán estar

---

68 Artículo 27.1 RLOPD: "*El derecho de acceso es el derecho del afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que se esté realizando, así como la información disponible sobre el origen de dichos datos (…)*".

69 BATUECAS CALETRÍO, Alfredo. "Intimidad personal, protección de datos personales y geolocalización"*,* cit., p.74.

70 BATUECAS CALETRÍO, Alfredo. "Intimidad personal, protección de datos personales y geolocalización", cit., p.74.

acompañadas de los datos exactos a que se refieren. Y el derecho de supresión trataría aquel supuesto en el que se eliminan aquellos datos inadecuados o excesivos, como regula el artículo 31.2 RLOPD[71].

El titular de la aplicación de geolocalización tiene la obligación de resolver la solicitud de rectificación y supresión –en la antigua Ley Orgánica de 15/1999 se denominaba derecho de cancelación- en un plazo máximo de diez días desde la recepción de la solicitud por parte del interesado. En el momento que transcurre el plazo sin que de forma expresa se haya respondido a la petición, el interesado tiene la posibilidad de interponer una reclamación ante la AEPD y ésta derivarlo al delegado de protección de datos, según se establece en el artículo 37.2 LOPDGDD. En el caso de que los datos rectificados hubieran sido cedidos previamente, el titular de la aplicación de geolocalización debe comunicar esta rectificación al cesionario, en el mismo plazo que para la resolución de la solicitud, para que proceda a la rectificación o cancelación de los datos (artículo 17 RLOPD).

Al ejercitar el derecho de oposición[72] (artículo 18 LOPDGDD, en relación con arts. 34 a 36 RLOPD), el titular de los datos muestra su oposición a que estos sean tratados. El ejercicio del derecho de oposición en el ámbito de las aplicaciones de geolocalización será muy residual, ya que este derecho se configura fundamentalmente para ejercitarlo en casos en los que no es necesario recabar el consentimiento del interesado para el tratamiento de sus datos. Este supuesto no se produce cuando se utilizan aplicaciones de geolocalización en las que, como se ha visto, la prestación del consentimiento es requisito necesario para el tratamiento de los datos de posicionamiento. Tendrá sentido el ejercicio de este derecho, por ejemplo, cuando se estén tratando datos de posicionamiento a consecuencia de que la aplicación de geolocalización estuviera activada en el terminal de forma premeditada[73].

---

[71] Artículo 17 RGPD: "*El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales (…)".*

[72] Art. 34 RLOPD: "*El derecho de oposición es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los siguientes supuestos: a) Cuando no sea necesario su consentimiento para el tratamiento (…); b) Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad (…); c) Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado (…)*".

[73] BATUECAS CALETRÍO, Alfredo. "Intimidad personal, protección de datos personales y geolocalización", cit., p. 75.

En este caso, el titular de la aplicación de geolocalización tiene como plazo máximo para resolver la solicitud de oposición diez días desde su recepción. En el momento que transcurra este plazo sin la respuesta a la petición de forma expresa, el interesado podrá interponer una reclamación ante la AEPD y ésta derivarlo al delegado de protección de datos, según se establece en el artículo 37.2 LOPDGDD.

Para que se puedan ejercer correctamente los derechos aquí mencionados, el titular de la aplicación de geolocalización facilitará al interesado un medio sencillo y gratuito para ello, (artículo 24.2 RLOPD). Los derechos de acceso, rectificación, supresión –denominado derecho de cancelación en la LO 15/1999- y oposición son derechos independientes, por lo que su ejercicio no está condicionado por el ejercicio previo de ninguno de los otros.

A modo de ejemplo, puede recordarse cómo se suscitó uno de los más grandes escándalos a nivel de protección de datos personales cuando Toysmart.Com, la compañía propiedad de Disney, al caer en bancarrota, anunció la venta de la información personal de sus clientes, incluyendo su nombre, dirección, información bancaria y familiar, sin que las personas cuyos datos se negociaban tuvieran derecho alguno a oponerse a la venta o a ser informados. Esto provocó un maremoto de reacciones en pro de proteger la privacidad, al ser una de las condiciones implícitas del tratamiento de los datos originariamente obtenidos el uso confidencial de la información (más viéndose involucrados menores). Ello condujo a que muchas empresas virtuales modificaran sus políticas de privacidad a fin de evitar futuros conflictos legales, entre ellas Amazon y eBay (pese a las protestas de muchos de sus usuarios), que incluyeron la posibilidad de divulgación y cesión de los datos personales que se les facilitaran. Con ello se ve que la modificación operada en las políticas de privacidad y condiciones de uso de las sociedades virtuales no fueron precisamente las más protectoras de dicha privacidad en un marco local que lleva a la autorregulación y en el que siempre se impone la ley del más fuerte[74].

De aquí van surgiendo todas aquellas reivindicaciones que exigen la configuración, junto al derecho a la vida privada, de un derecho al olvido digital, al anonimato y a la desconexión; derechos que deben tener una viabilidad jurídica y técnica. El 17 RGPD es el que regula hoy el derecho de supresión, también llamado "derecho al olvido". Como ya hemos visto, "*un interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los*

[74] BARINAS UBIÑAS, Désirée. El impacto de las tecnologías de la información y de la comunicación en el derecho a la vida privada, cit., pp. 49-50.

*datos personales que le conciernan*". El responsable estará obligado a suprimir los datos cuando concurra alguna de las circunstancias siguientes:

1. Cuando los datos personales no sean necesarios para los fines para los que se hayan recogido.

2. Cuando el sujeto interesado retire el consentimiento en el que se basa el tratamiento "*conforme a los artículos 6.1.a), o el artículo 9.2.a)*".

3. Cuando el interesado se oponga al tratamiento (artículo 21.1 LOPDGDD) y no existan motivos legítimos para seguir con el mismo, o cuando se oponga al tratamiento de los datos que han sido tratados ilícitamente (artículo 21.2 LOPDGDD).

4. Aquellos datos tratados de una manera ilícita.

### *3.3.2. Geolocalización en el ámbito laboral: intimidad vs ámbito empresarial.*

Como hemos estado estudiando, un geolocalizador es un instrumento que permite establecer la posición de un dispositivo electrónico. Se puede obtener incorporándolo en un sistema de geolocalización, como por ejemplo el GPS que tenemos integrado en nuestros dispositivos electrónicos, ya sea el teléfono móvil o una Tablet.

Por otra parte, en el ámbito laboral, aparte de los dispositivos cotidianos que acabamos de ver y que todos llevamos en nuestro día a día, existe un dispositivo específico que es el tacógrafo, por el que se registra de una manera continuada todos los datos relativos al movimiento del vehículo donde se sitúa, o porque el trabajador lo lleve consigo durante su jornada laboral.

Sin duda que el recurso empresarial a este tipo de dispositivos puede tener una justificación organizativa, técnica o productiva en términos de eficiencia, de control y de seguridad. Es así respecto de prestaciones de servicios que se desarrollan fuera de los centros de trabajo para las que la utilización de geolocalizadores sirve para una mejor y más eficiente prestación laboral al permitir, por ejemplo, asignar tareas en razón de la situación concreta del trabajador por tratarse de destinatarios de servicios ubicados en su entorno (el supuesto

de trabajadores dedicados a reparto, mantenimiento y reparación, instalación o cualquier tipo de servicio técnico a prestar en el domicilio del cliente o en el lugar donde éste se encuentre)[75].

En este punto, podemos comentar la Sentencia de la Audiencia Nacional, Sala de lo Social, Sección 1ª, Sentencia 13/2019, de 6 Feb. 2019 (AN 2019\905) relativa a la imposición, por parte de la empresa Telepizza, de un sistema de geolocalización denominado "Tracker"; aplicación que deben descargar en sus teléfonos móviles todos sus empleados que se ocupen de repartir la comida. Los representantes de los trabajadores recriminan a la empresa que este método de geolocalización incumple el deber de información y consulta a sus empleados, y que se vulnera el derecho a la privacidad al no superar el juicio de proporcionalidad entre el uso de este sistema y la intimidad de cada empleado[76].

El Tribunal Supremo, Sala de lo Social, Sección 1ª, Sentencia 163/2021, de 8 febrero 2021 (RJ 2021\672), se ha pronunciado también sobre este asunto. Este Tribunal confirma la existencia de otros métodos para ejecutar la geolocalización con una menor injerencia en los derechos fundamentales de los trabajadores de la empresa Telepizza; aparte, con este sistema de geolocalización, se entromete en los datos personales de los empleados como, por ejemplo, el número de teléfono o la dirección de correo electrónico.

El TS se basa en que el proyecto "Tracker" afecta al sistema de organización y control del trabajo, a pesar de que su finalidad sea la de facilitar al cliente el seguimiento de su pedido. También existe un abuso de derecho porque, en el caso de que el móvil sufra alguna alteración que no permita la conexión, la responsabilidad pasa al trabajador, llegando incluso a ocasionar la pérdida de salario o de su puesto laboral. Además, este proyecto fue implantado por la empresa de una manera unilateral, es decir, sin haber informado a los representantes de los trabajadores.

La Sala de lo Social no niega que este proyecto pueda ser una medida legítima para determinados fines o que se pueda evitar un déficit comercial competitivo; pero, en su

---

[75] GONZÁLEZ ORTEGA, Santiago. Las facultades de control a distancia del trabajador: geolocalizadores y tacógrafos, cit., p. 48.

[76] Se acusa a la empresa de la utilización de un sistema de geolocalización que vulnera el derecho de intimidad de sus repartidores, porque se les obliga a "*aportar a la actividad empresarial de un teléfono móvil con conexión a Internet, y ésta aplicación permite la geolocalización del dispositivo y del trabajador durante su jornada laboral*".

implantación, no supera los criterios constitucionales ni legales (art. 38 CE y art. 1.1 y art. 5.c) ET), existiendo otros métodos para ejecutar este sistema con una menor injerencia en los derechos fundamentales de los trabajadores y, por consiguiente, sin intromisión en los datos de carácter personal.

El uso de los dispositivos de geolocalización y los tacógrafos tienen una utilidad empresarial, y un fundamento constitucional y legal (artículo 38 CE[77], artículo 20.3 ET[78] y artículo 90 LOPDGDD[79]), pero ello no significa que la empresa pueda instalar este tipo de dispositivos sin ningún tipo de motivación ni consentimiento. La implantación y uso de este tipo de dispositivos y/o herramientas empresariales tienen ciertos límites que derivan de la condición de datos que están vinculados con el trabajador y que pueden ser clasificados como informaciones que han sido obtenidas en el ámbito empresarial, y que deben respetar los derechos recogidos en el artículo 18 de la CE[80].

Aunque podría sostenerse que los datos proporcionados por los dispositivos de geolocalización y por los tacógrafos no son, en principio y de forma directa, datos personales ya que se refieren a la ubicación y al movimiento del propio dispositivo, sin embargo, la amplia definición de dato personal permite concluir lo contrario. Así lo justifica la mención

---

[77] Artículo 38 CE: "*Se reconoce la libertad de empresa en el marco de la economía de mercado. Los poderes públicos garantizan y protegen su ejercicio y la defensa de la productividad, de acuerdo con las exigencias de la economía general y, en su caso, de la planificación*".

[78] Artículo 20.3 ET: "*El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad (…)*".

[79] Artículo 90 LOPDGDD: "*1. Los empleadores podrán tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas (…). 2. Con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores (…)*".

[80] Artículo 18 CE: "*1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. 2. El domicilio es inviolable (…). 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial. 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar (…)*"

expresa a los datos de localización contenida en el artículo 4 RGPD en la medida en que se trata de datos que permiten la identificación de una persona concreta, vinculando a ella la información de ubicación, movimiento y actividades que tales datos reflejan. Y lo da por descontado, sin mayores precisiones y respecto de los trabajadores asalariados, el ya citado artículo 90 LOPDGDD, el cual somete a las reglas de la norma, que tiene como objetivo el *tratamiento de los datos personales, los datos de los trabajadores obtenidos mediante sistemas de geolocalización*[81].

Por ello, los datos que se recopilan deben limitarse a lo estrictamente necesario para lograr la finalidad empresarial. En este sentido lo debemos relacionar con los modos de control de los trabajadores como, por ejemplo, la geolocalización, que no puede ser un objetivo en sí mismo, sino exclusivamente una consecuencia de una medida necesaria e imprescindible para garantizar el buen funcionamiento de la empresa, y para proteger la producción, la salud y la seguridad.

Por el contrario, existen sistemas de localización que, aunque a priori parezca que vulneran nuestra intimidad, han sido importantes para realizar un despido a una trabajadora por hacer un uso inadecuado del vehículo de la empresa. En este sentido la STS 766/2020, Sala Cuarta, de lo Social, 15 de septiembre de 2020, Rec. 528/2018 (RJ 2020\4005), que trata sobre un despido disciplinario. El Tribunal Supremo casa la sentencia del TSJ, que consideró improcedente el despido de una empleada que utilizó el coche de la empresa durante una baja y el descanso laboral. Se tiene constancia de este uso a través de los datos que arroja el GPS instalado en el vehículo, pero el Tribunal considera que no se vulnera la intimidad del trabajador porque no se revelaban datos personales; además, la trabajadora conocía las normas internas que prohibían dicha conducta.

Como acabamos de estudiar y para finalizar esta pequeña referencia al ámbito laboral, toda empresa que vaya a utilizar sistemas de localización entre sus empleados, deberá hacer constar estos dispositivos en el contrato del trabajador, haciendo mención especial del tipo de sistema de localización que se vaya a utilizar y su finalidad. Por otra parte, toda empresa

[81] GONZÁLEZ ORTEGA, Santiago. Las facultades de control a distancia del trabajador: geolocalizadores y tacógrafos. *Revista andaluza de trabajo y bienestar social*. Nº 150/2019. Monográfico sobre las facultades de control empresarial ante los cambios tecnológicos y organizativos (ISSN: 0213-0750), pp. 45-71. Pág. 50.

deberá dar a este sistema de localización el uso exclusivo para el que se instaló y así evitar la intromisión en la intimidad del empleado. Pero no debemos olvidar que el trabajador tampoco debe excederse en su puesto de trabajo y utilizar los dispositivos para uso personal, o los vehículos donde llevan integrados algún sistema de localización, como, por ejemplo, un GPS, para usos cotidianos que no tienen ninguna relación con su trabajo y lo utilizan fuera de su jornada laboral.

### *3.3.3. Consecuencias en la utilización de las Redes sociales.*

Como es sabido, en el momento que subimos una foto a una Red social, o simplemente escribimos un tweet sobre cómo nos ha ido el día o sobre si estamos a favor o en contra de que haya ganado un partido de futbol nuestro equipo favorito, todos esos datos se recolectan para hacer una radiografía de nuestros gustos y así las páginas Web nos pueden mostrar aquellas direcciones que puedan ser de nuestro interés, todo ello relacionado con lo que nosotros exponemos en las Redes sociales.

Lo más importante, y lo que nos debe preocupar, es que, aunque, cuando una persona es mayor de edad y empieza a tener más conciencia de que las Redes sociales y exponer datos de su vida privada, pueden conllevar una exposición excesiva de nuestra vida privada e intimidad, existen usuarios que no tienen esta conciencia y son los menores, que no son conscientes de que todo lo que suban deja de ser de su propiedad e, incluso, en alguna ocasión con la persona que ellos creen que hablan no es en realidad ese usuario, sino que se esconde detrás de una identidad falsa.

Esta captación de datos tiene trascendencia respecto de la privacidad, ya que las plataformas disponen de potentes herramientas de procesamiento y análisis de los datos facilitados por los usuarios. Además, a ello se añade la circunstancia de que, en múltiples Redes, los perfiles de los usuarios aparecen indexados en determinados buscadores de Internet, así como que se detecta, en términos generales, una ausencia de mecanismos que permitan controlar la edad de las personas que se conectan a las Redes y evitar que accedan

los menores de 14 años sin el preceptivo consentimiento o autorización de los padres o tutores, tal como determina el artículo 13.1 y 13.4 del RLOPD[82].

El problema principal que ocasiona Facebook, por ejemplo, es que los usuarios de esta Red social no sólo exponen sus datos, sino que además publican sus vivencias; por lo tanto, el ámbito de la privacidad se abre de forma exponencial con la consecuencia de un aumento del riesgo de atentados contra los derechos de la personalidad, incrementándose incluso los ilícitos penales.

#### *3.3.3.1. Baremo de restricciones según la edad.*

En el caso de las restricciones por edad dentro de las Redes sociales, es cierto que la mayoría de las plataformas prohíben el registro de menores de 13 años, recomendando para su uso el permiso de los progenitores para aquellos usuarios entre 14 y 18 años. Pero existe la incertidumbre de cómo se puede tener conocimiento de que estas restricciones se llevan a cabo si en realidad no existen pruebas fehacientes de la edad de las personas que se suscriben en la plataforma.

Los menores, aquel grupo de usuarios de 13 años o inferior, se ven expuestos a interactuar con personas adultas, que, en alguna ocasión, van con malas intenciones, haciéndose pasar por otros menores para así convertirse en sus amigos. Todo ello lo podemos ver en el ejemplo del *child grooming* o acoso de menores por Internet, en el que las Redes sociales e Internet juegan un papel fundamental.

Los menores de 14 años pueden acceder a diversas informaciones que pueden no ser aptas para su edad y se exponen a entrar en un mundo "virtual" del que desconocen sus consecuencias, y, por lo tanto, son más propensos a ignorar los riesgos que acarrean las Redes sociales.

[82] GIL ANTÓN, Ana María. *El derecho a la propia imagen del menor en internet*. España: Dykinson, 2014, pp. 93-95. Pág. 94.

Haciéndonos eco de los principales peligros identificados por la Agencia Española de Protección de Datos y el Instituto Nacional de Tecnologías de la Comunicación (INTECO) en el estudio realizado sobre las Redes sociales, señalamos los siguientes:

- La exposición de datos que pueden considerarse como sensibles.
- La falta de conciencia de los usuarios de que sus datos pueden ser accesibles a cualquier persona y de su valor en el mercado.
- La manipulación de los datos por terceros malintencionados.
- La publicación de información sin autorización de la persona, que puede serle perjudicial, tanto de personas usuarias como no usuarias del servicio.
- Las condiciones de registro que permiten una recolección y explotación comercial, prácticamente ilimitada, por parte de los proveedores del servicio[83].

Existe un tipo de recolección secundaria de los datos personales de los usuarios, y que éstos normalmente desconocen, por la que se pueden personalizar los perfiles de éstos de manera más exhaustiva; la cesión de los datos personales a terceros desconocidos cuyo tratamiento y control se desvincula de los afectados; la suplantación de identidad –delito tipificado en el artículo 401 del Código Penal-; y en el caso de los menores, la exposición de su imagen y datos personales sin ser conscientes de todo el alcance que pueda conllevar.

Otro efecto negativo cuando nos damos de alta en una Red social es que podemos tener conocimiento de que otra persona nos ha usurpado nuestra identidad, es decir, se ha creado un perfil con todos nuestros datos, haciéndose pasar delante de otros usuarios como si fueran nosotros mismos.

En la actualidad, existe una problemática con este tipo de usurpación dentro del ámbito de los menores, ya que se puede dar la circunstancia de que un acosador, ya sea mayor de edad o menor, se cree un perfil falso para ganarse la confianza de un usuario menor de edad –normalmente, son los más vulnerables en este aspecto- y, posteriormente, cuando gane más confianza, pueda involucrarle en una actividad sexual como, por ejemplo, hacerse con imágenes de contenido pornográfico. Esta es una conducta penalmente castigada, denominada *Grooming*, en el artículo 183 ter CP, que diferencia, por un lado, entre aquellos

[83] BARINAS UBIÑAS, Désirée. El impacto de las tecnologías de la información y de la comunicación en el derecho a la vida privada, cit., p.36.

contactos que se realicen a través de Internet o cualquier otra tecnología de la información y la comunicación, con un menor de dieciséis años cuando el acosador proponga un encuentro con la víctima para cometer aquellos delitos regulados en los artículos 183 y 189 CP, lo que se castigará "*con la pena de uno a tres años de prisión o multa de doce a veinticuatro meses (…)*" (primer párrafo del artículo citado). Por otro lado, el párrafo segundo de este artículo, regula aquellos casos en los que se realicen actos dirigidos a embaucar a la víctima para que ésta facilite material de tipo pornográfico o muestre imágenes comprometidas en las que aparece un menor, lo que "*será castigado con una pena de prisión de seis meses a dos años*".

# 4. LA REALIDAD DEL RADAR COVID EN TIEMPOS DE PANDEMIA.

## 4.1. Uso del Radar Covid.

Para entender el nacimiento y la función del Radar-Covid, debemos hacer una pequeña introducción acerca del momento histórico que estamos viviendo.

Como ya sabemos, a finales del 2019 se empezó a propagar por todo el mundo un virus muy contagioso y letal, que finalmente se convirtió en una pandemia mundial, dejando millones de fallecidos y muchas personas con secuelas graves derivadas del Covid-19.

El día 28 de marzo de 2020 el Ministerio de Sanidad, a través de la Orden SND/297/2020, delegó en la Secretaría de Estado de Digitalización e Inteligencia Artificial para que desarrollasen una aplicación móvil denominada "Asistencia Covid-19". Gracias a esta Orden se pudo realizar un estudio sobre la movilidad de la población a través de los datos recabados por los dispositivos móviles.

Después de que un ciudadano se realiza una prueba PCR o de antígenos, puede publicar sus resultados dentro de la aplicación. A través de un cuestionario que debe realizar sobre su información personal –nombre, apellidos, número de teléfono móvil, DNI, para así derivarlo con la tarjeta sanitaria, y, por último, su fecha de nacimiento y dirección-.

A continuación, y a modo de ejemplo práctico de esta nueva aplicación que nos ha estado acompañando durante un tiempo, iré explicando poco a poco su funcionamiento acompañado de imágenes para que así sea más didáctico.

En primer lugar, cuando vamos a la aplicación de descargar de nuestro teléfono móvil, lo primero que vemos, cuando buscamos la aplicación de Radar Covid, es un mensaje que expone: "*Recibirás una alerta cuando estés cerca de alguien que ha informado de que tiene el Covid-19. Esta aplicación está autorizada por España y usa el sistema de notificaciones de exposición de Apple y Google. Toca para ver otras aplicaciones de seguimiento de contactos*"[84]. Por tanto, lo primero que se explica es la utilidad de esta aplicación, que es que se nos informe en caso de haber estado cerca de una persona infectada por el virus. Será de mucha ayuda que recibamos esta información, ya que somos personas que nos vamos al trabajo, a bares, a clase, etc., en

[84] Véase Imagen núm. 1.

definitiva, que socializamos, por tanto, es útil, en estos momentos, que, si en algún sitio que hayamos estado ha pasado algún infectado, que tengamos conocimiento sobre ello para tomar las medidas necesarias.

Después, nada más instalar esta aplicación sale un pequeño mensaje explicando el significado y el instrumento del Radar Covid[85]. A continuación, vemos otra pantalla con el título "*Tu privacidad es nuestra prioridad*"[86]; esa privacidad que hemos ido defendiendo en todo este trabajo en virtud de la cual los usuarios tienen derecho a ser conscientes de qué tipo de datos van a ser utilizados y los fines concretos. Si no estamos conformes con la política de privacidad y las condiciones de uso, no podremos utilizar esta aplicación.

- En cuanto a la POLÍTICA DE PRIVACIDAD: Nos explican qué es el Radar Covid; su funcionamiento; la transferencia de datos a países de la Unión Europea para una mayor identificación de los usuarios en caso de que hayan viajado o hayan estado con un visitante procedente de otro país; y los responsables del tratamiento de nuestros datos como usuarios de esta aplicación –que serán tanto el Ministerio de Sanidad como las Comunidades Autónomas y la Secretaría General de Administración Digital-.

  Aquí debemos atender al artículo 11.1 y 2 LOPDGDD, que regula la transparencia e información al afectado. Comparando la información que tenemos sobre quiénes son los responsables de esta aplicación, y lo que regula este artículo, este apartado está acorde a la Ley.

  Un apartado que nos interesa es el de los datos que van a ser tratados sobre nosotros, donde se especifica que no se permitirá la identificación directa del usuario o del teléfono, y sólo serán tratados aquellos datos necesarios para informar al usuario de que ha estado expuesto a una situación de riesgo de contagio por el Covid-19, así como para la adopción de medidas necesarias en estos casos de infección.

  Toda la información que es recogida será estrictamente por interés público en el ámbito de la salud y, ante esta situación de emergencia decretada con el fin de

[85] Véase Imagen núm. 2.
[86] Véase Imagen núm. 3.

proteger el interés esencial de la vida de los ciudadanos, debemos atender a los artículos 6.1.a), c), d) y e), y a los artículos 9.2.a), c), h) e i) RGPD.

En relación con el artículo 6.1 RGPD, los apartados que serían adecuados en este supuesto del Radar Covid, a mi juicio, serían el d), relativo al tratamiento que es *necesario para la protección de intereses vitales*, ya que la misión principal es protegernos a nosotros y a la sociedad en la medida de lo posible. Otro apartado que considero relevante es el e), en tanto que esta aplicación ha sido creada y/o tiene una misión de interés público, para intentar controlar los brotes que se den en un determinado lugar.

Más concretamente, en el artículo 9 RGPD dedicado al tratamiento de categorías especiales de datos personales, entre los que se incluyen los de salud, los apartados que considero más relevantes, para justificar en este caso el tratamiento, son el h), que lo autoriza cuando tenga una finalidad médica preventiva; la función única del Radar Covid es médica y que todo ciudadano que se descargue la aplicación pueda conocer si ha estado con algún infectado de Covid-19 y así poder tomar las medidas necesarias para no contagiar a su círculo familiar y de amistad. Y, por supuesto, también el apartado i) porque el tratamiento de estos datos tiene un *interés público en el ámbito de la salud pública*; en particular, como señala la propia norma, la protección frente a amenazas que superen las fronteras y sean consideradas graves para la salud –este apartado tiene relación directa con la pandemia generada por el Covid-19 que afecta a nivel mundial, y que todos los países han estado intentando controlar para que no se propagase, en la medida de lo posible, a otros países-.

Otra cuestión de gran interés es el tiempo de conservación de nuestros datos. En esta política de privacidad se expone que las claves de exposición temporal y los identificadores efímeros del Bluethooth son almacenados en nuestro dispositivo durante un tiempo de 14 días; a partir de ahí serán eliminados. Esta limitación del

tiempo de conservación de los datos viene exigida en los artículos 5.1.e) y 89.1 RGPD[87] y en el artículo 89.1[88].

Por supuesto, y como hemos expuesto en un epígrafe, en esta aplicación todos los usuarios tienen una serie de derechos, concretamente los derechos de acceso, rectificación, supresión, limitación y oposición –todos ellos vistos y explicados anteriormente-.

Una normativa nueva que nosotros no hemos utilizado hasta ahora en el trabajo y esta aplicación sí, será el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Con esta normativa se pretende regular aquellas medidas de seguridad que utiliza esta aplicación que están previstas en el Anexo II (Medidas de seguridad[89]) de dicho Real Decreto.

Para terminar, explica la edad mínima para la utilización de esta aplicación –que será de 18 años- y la calidad de los datos que se deben proporcionar por parte del usuario, es decir, que, para un uso más satisfactorio, la información deberá ser real, veraz y actualizada.

Por último, encontramos un concepto que ha sido explicado anteriormente, "*cookies*"; aquí será utilizada esta técnica para permitir al usuario la navegación y utilización de diferentes opciones o servicios que ofrece esta aplicación como, por

---

[87] Artículo 5.1.e) RGPD: "*mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales (…)*".

[88] Artículo 89. 1 RGPD: "*El tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos estará sujeto a las garantías adecuadas (…). Dichas garantías harán que se disponga de medidas técnicas y organizativas, en particular para garantizar el respeto del principio de minimización de los datos personales. Tales medidas podrán incluir la seudonimización (…)*".

[89] Anexo II Real Decreto 3/2010: "*1. Para lograr el cumplimiento de los principios básicos y requisitos mínimos establecidos, se aplicarán las medidas de seguridad indicadas en este anexo, las cuales serán proporcionales a: a) Las dimensiones de seguridad relevantes en el sistema a proteger; b) La categoría del sistema de información a proteger*".

ejemplo, entrar a un acceso restringido –cuando entramos en una Página Web, en ocasiones, nos sale un mensaje que pone "*Esta web utiliza cookies propias y de terceros para su correcto funcionamiento y para fines analíticos. Al hacer clic en el botón Aceptar, acepta el uso de estas tecnologías y el procesamiento de sus datos para estos propósitos*"; en este caso, cuando aceptamos la utilización de las cookies, tendremos un acceso libre a la página, que anteriormente no teníamos-. Para ver toda la lista de Política de Privacidad de esta aplicación se puede entrar a esta Página Web: https://radarcovid.gob.es/politica-de-privacidad

- En las CONDICIONES DE USO: Nos vuelven a explicar en qué consiste esta aplicación, su funcionamiento y, dentro de éste, nos explica los efectos que tiene la activación de la aplicación en el momento que el usuario acepta: a) envío de señales Bluetooth emitidas de forma anónima por su dispositivo; b) la recepción y almacenamiento de señales Bluetooth de aplicaciones compatibles con Radar Covid, que se mantienen de forma anónima y descentralizada en los dispositivos de los usuarios durante un periodo no superior a 14 días; c) la información ofrecida al usuario sobre el posible riesgo de contagio, sin que en ningún momento se refieran datos personales de ningún tipo; d) recibir claves positivas de terceros países de la UE a través de la plataforma de interoperabilidad de la UE (EFGS); e) bajo consentimiento explícito, el envío de claves positivas que serán compartidas con terceros países de la UE a través de la plataforma de interoperabilidad de la UE (EFGS)[90].

  Por supuesto, en el ámbito de seguridad y privacidad, nos vuelve a remitir al Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, anteriormente comentado.

En la siguiente imagen[91], nos vuelve a explicar de una manera más breve el funcionamiento de la aplicación. En primer lugar, tener activado el Bluetooth; en caso de que

[90] Condiciones de uso de Radar Covid (2021), véase https://radarcovid.gob.es/condiciones-de-uso [Última visualización: 24/06/2021]

[91] Véase Imagen núm. 4.

seamos positivo en Covid-19, debemos introducir aquí un código que nos facilitarán las autoridades sanitarias y, por último, en caso de que hayamos tenido contacto estrecho con un infectado, recibiremos un mensaje. Cuando damos a continuar en esta página, nos sale un mensaje donde pone "*Radar Covid quiere activar el Bluethooth*", que deberemos aceptar para que se ponga en funcionamiento esta aplicación.

A continuación, nos preguntan si queremos activar las notificaciones de exposición al Covid-19; después, necesitamos activar los ajustes de ubicación del dispositivo, si bien se explica que este sistema de notificaciones de exposición no usa, ni guarda, ni comparte la ubicación de nuestro dispositivo como el GPS[92]. En este punto, llegamos al final de la instalación de la aplicación[93], en mi caso, y como podemos ver en la imagen, al descargarlo ahora mismo informa que he estado sin contactos de riesgo y que tengo el Radar Covid activado.

Como curiosidad, en la pantalla principal que se nos queda cuando hemos terminado de instalar la aplicación, encontramos dos casillas con datos relevantes:

1. En cuanto a la casilla relativa "*mis datos*"[94], de nuevo se nos hace un pequeño resumen de la privacidad de esta aplicación donde se explica que no recoge ningún dato personal ni ningún dato de geolocalización, por tanto, no se podrá determinar ni nuestra identidad ni la de las personas con las que estemos.

2. En la casilla "*estadísticas de Radar Covid*" nos vienen una serie de datos interesantes para conocer si de verdad ha sido útil y se utiliza esta aplicación, ya que aquí nos dice el número de descargas que ha tenido el Radar Covid; casos positivos declarados en RADAR Covid desde el 19/08/2020; y los países conectados con Radar Covid[95]. Para ver con más detalle estas estadísticas hay que entrar en esta Página Web: https://www.radarcovid.gob.es/estadisticas/descargas-radar

[92] Véase Imagen núm. 5.
[93] Véase Imagen núm. 6.
[94] Véase Imagen núm. 7.
[95] Véase Imagen núm. 8.

# 5. CONCLUSIONES.

A lo largo de este trabajo hemos ido analizando los aspectos más relevantes de la legislación de protección de datos, sobre todo, en relación con las Redes sociales, instrumentos que, en la actualidad, ha pasado a formar parte de nuestras vidas.

Hemos estado estudiando si, en los tiempos que estamos viviendo, las Redes sociales o todas las nuevas tecnologías que nos rodean vulneran, o no, nuestra privacidad. Tal y como expuse en la Introducción, el derecho a la intimidad se podría equiparar, dentro de las estancias de una casa, al dormitorio y al baño, pero la privacidad aún va más allá; pues bien, tal y como hemos señalado a lo largo del trabajo, toda la legislación que regula la protección de datos, ya sea a nivel nacional como a nivel de la Unión Europea, establece una serie de límites que para aquellas entidades o contratantes que quieran tratar determinados datos de los interesados. Pero lo más relevante y, por supuesto, sobre lo que se basa esta regulación es el consentimiento del interesado, es decir, sin que éste preste un consentimiento, previa una información clara y específica, se entenderá ilícito el tratamiento de los datos. Aunque también debemos mencionar que existen tratamientos lícitos de datos que no necesitan el consentimiento expreso del interesado –como es el supuesto de tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos (artículo 7 LOPDGDD), y el tratamiento de datos relativos a condenas e infracciones penales (artículo 10 RGPD).

Tampoco debemos olvidar que, para salvaguardar nuestro derecho a la intimidad, la Ley de Protección de Datos regula una serie de derechos que tienen aquellos los afectados para defender sus intereses.

Es cierto que hoy en día Internet es una gran herramienta para la vida cotidiana, lo utilizamos para todo, ya sea para trabajar, hacer la compra, o por entretenimiento; pero como todo, tiene "su cara y su cruz", por tener acceso a mucha y muy variada información debemos pagar un alto precio, nuestros datos.

Ya hemos visto que existen unos datos personales específicos que no pueden ser tratados, por ejemplo, nuestra ideología política, orientación sexual, etc., pero considero que existen otros datos que, a pesar de que se pueden utilizar y recabar, olvidamos que sí se pueden considerar íntimos y que, en estos momentos, los compartimos sin ser del todo conscientes de la repercusión que puedan tener en Internet.

Por nuestra experiencia, uno de los datos que hacemos públicos en Internet es nuestro correo electrónico, necesario para tener una cuenta en Google y "navegar" por diferentes

páginas. A raíz de dar acceso a este dato, cuando buscamos algo, ya sea para irnos de viaje o comprar algún producto, se nos va a relacionar con una serie de páginas donde se encontrarán algunos productos que nos puedan gustar derivados de las búsquedas que hayamos realizado. Y todo ello estará conectado con nuestro correo electrónico y, por lo tanto, se sabrá que nosotros, como personas físicas, tenemos unos gustos determinados y las empresas podrán estudiarlos y hacer publicidad de sus productos.

Lo que más me llama la atención es que Internet y las Redes sociales sean tan esenciales en nuestras vidas, formen una parte tan fundamental de la sociedad que ahora mismo sería imposible convivir sin ellas. No digo que la época anterior a Internet fuese mejor, creo que ahora tenemos mayor accesibilidad a los datos y de una manera más cómoda, pero es cierto que estamos dejando la vida "física" por una "virtual"; es simple, sólo hay que ver que la mayoría de las personas, en estos momentos, habrá comprado, al menos, un producto a través de alguna Página Web.

Es por ello que los dispositivos móviles siempre estarán con nosotros y esta será la vía para nuestra geolocalización; por eso, estamos siempre localizados, sin un ápice de intimidad. A lo largo del trabajo hemos hecho mención a la localización dentro de la empresa, donde hemos realizado un estudio sobre los límites que deben respetar las empresas con los trabajadores a fin de respetar el derecho a la intimidad de éstos. En el momento que un sistema de localización está siempre conectado con nosotros, tanto fuera como dentro de nuestra jornada laboral, se tratará de una vulneración del derecho a la intimidad, y todos y cada uno de nosotros merecemos intimidad y privacidad.

Todo esto lo podemos relacionar con el Radar Covid esta nueva aplicación de la que tanto hemos oído hablar este último año a raíz de la pandemia generada por el Sars-Cov-2. Debo empezar diciendo que era reacia a utilizar esta aplicación, ya que consideraba que vulneraba mi derecho a la intimidad por estar localizada en todo momento; pero, gracias a este trabajo de investigación y al estudio en profundidad que he hecho de la legislación relativa a la protección de datos, ahora mismo puedo decir que es una aplicación muy útil y que está perfectamente regulada.

Como hemos ido analizando en el apartado anterior, esta aplicación no utiliza el GPS de nuestro móvil para localizarnos, sino el Bluetooth. Tampoco nos ha pedido ningún dato relevante o íntimo de nosotros, sino que lo único que tendríamos que poner es un código que nos proporcionarían las autoridades sanitarias en caso de dar positivo en Covid-19; en mi caso, al ser negativa, no ha sido necesario inscribir este código.

Lo único deficiente que veo en esta aplicación son las pocas descargas que ha tenido, ya que, si fue creada para que la población la tuviese instalada en sus dispositivos móviles y así conocer si hemos estado cerca de algún infectado, si no hay un gran número de personas que lo utilicen, no podremos estar seguros de sí con quién hemos estado relacionándonos son positivos o negativos. Otro inconveniente que considero que existe, es la mala utilización que se ha podido realizar de este Radar, ya que nos pide un código que debemos introducir en caso de dar positivo, pero existe una parte de la población que no ha introducido ese código y ha seguido con su vida cotidiana, ya sea porque necesitan ir al trabajo ya que su situación económica está al límite, o simplemente porque no ha querido guardar la cuarentena.

Es una situación muy difícil de control y esto ya sobrepasa la legislación que regula el Radar Covid, es una cuestión de ciudadanía, pero, en lo que concierne a la aplicación, considero que es un buen método para controlar a los infectados y que se controlen aquellos brotes que se den en las ciudades.

Para terminar con mis conclusiones, sólo puedo decir que estamos protegido en lo relativo al tratamiento de nuestros datos, que no se pueden utilizar de una manera ilícita y que existen una serie de límites para su tratamiento. Pero me gustaría que dejásemos de lado tanta vida "virtual" y volviésemos a relacionarnos más de una manera física, que dejemos de conocer a gente vía Internet o hacer compras; que levantemos nuestra cabeza de las pantallas y disfrutemos de nuestra sociedad, de la gente, cuando estemos con nuestros amigos en un bar hablemos y pasemos el tiempo con ellos, y no que nuestro único fin sea hacer alguna foto con ellos y publicarlo en una Red social para que el resto de nuestros amigos virtuales vean que tenemos vida exterior, cuando, en realidad, sólo lo hacemos para la aprobación de esos amigos "virtuales".

# 6. ANEXOS.

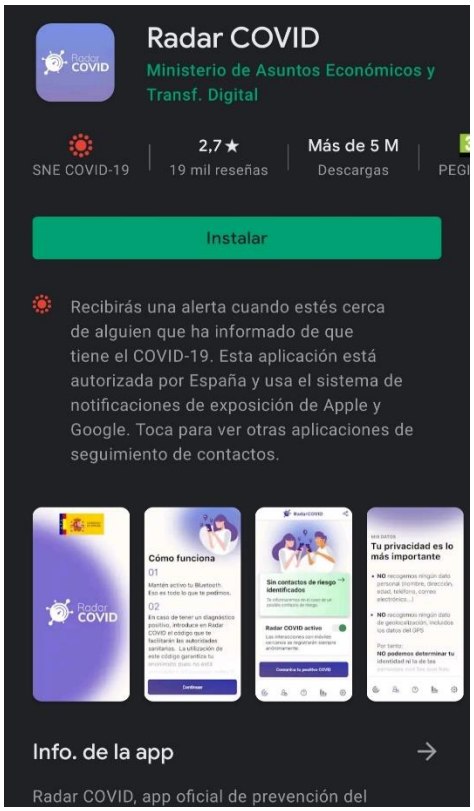


Imagen núm. 1.

Imagen núm. 2.

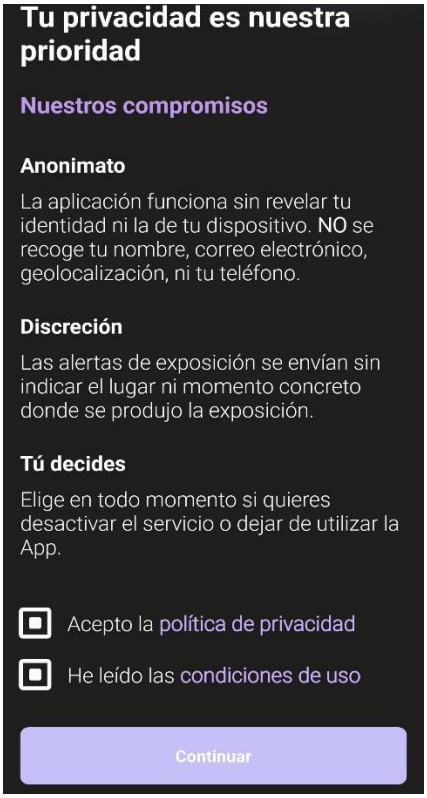


Imagen núm. 3.

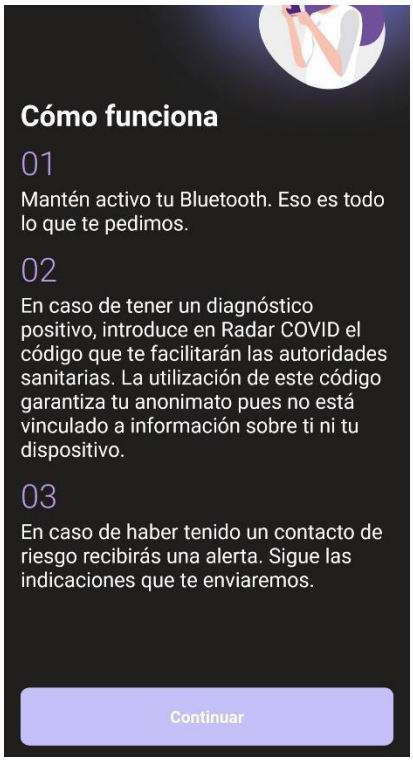


Imagen núm. 4.


RadarCOVID
Activa los ajustes de ubicación del dispositivo
Los ajustes de ubicación del dispositivo deben estar activados para que el Bluetooth pueda detectar dispositivos cercanos que tengan activadas las notificaciones de exposición. El sistema de notificaciones de exposición no usa, guarda ni comparte la ubicación de tu dispositivo, como el GPS.
Las aplicaciones que ya tenían permiso para usar la ubicación de tu dispositivo podrán acceder a ella de nuevo. Puedes ver y cambiar el permiso de ubicación de cualquier aplicación en Ajustes.
Atrás
Activar
Comunica tu positivo COVID

Imagen núm. 5.

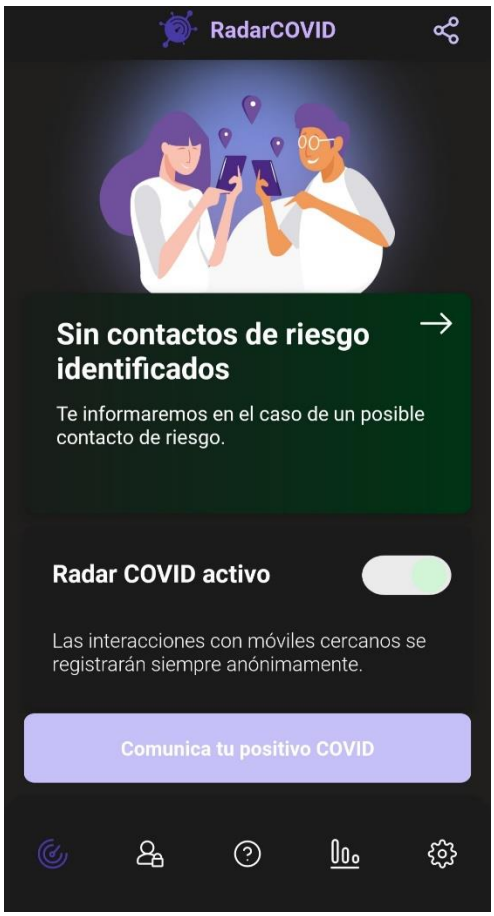
RadarCOVID
Sin contactos de riesgo identificados
Te informaremos en el caso de un posible contacto de riesgo.
Radar COVID activo
Las interacciones con móviles cercanos se registrarán siempre anónimamente.
Comunica tu positivo COVID

Imagen núm. 6.

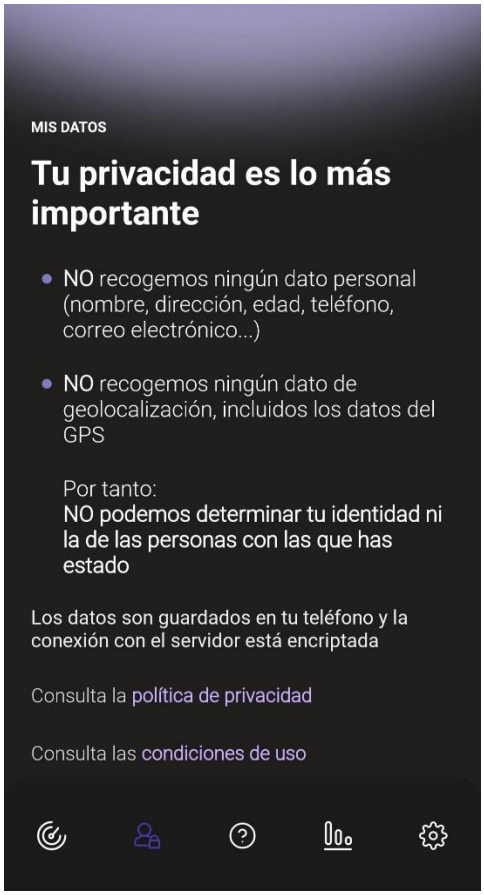


Imagen núm. 7


Imagen núm. 8.

# 7. BIBLIOGRAFÍA.

## 7.1. Artículos de revistas y capítulos de libros.

### *7.1.1. Artículos de revistas.*

BARINAS UBIÑAS, Désirée. El impacto de las tecnologías de la información y de la comunicación en el derecho a la vida privada. *In Revista electrónica de ciencia penal y criminología* (Issue 15), núm. 15, 2013, pp. 01-60.

BATUECAS CALETRÍO, Alfredo "Intimidad personal, protección de datos personales y geolocalización" *Personal Privacy, Personal Data Protection and Geolocation Apps*, núm. 29, 2015, pp. 47-82.

CASTELLANOS MEJÍA, Juan Camilo y MONTEZUMA CHÁVEZ, Luis Alberto. "El uso de sistemas de localización en las plataformas de comunicación en línea o en las Redes sociales". *Revista de Derecho Comunicaciones y Nuevas Tecnologías,* núm. 16, 2016, pp. 01-27.

### *7.1.2. Capítulos de libros.*

GIL ANTÓN, Ana María. *El derecho a la propia imagen del menor en internet*. España: Dykinson, 2014, pp. 93-95.

GONZÁLEZ ORTEGA, Santiago. Las facultades de control a distancia del trabajador: geolocalizadores y tacógrafos. *Revista andaluza de trabajo y bienestar social.* Nº 150/2019. Monográfico sobre las facultades de control empresarial ante los cambios tecnológicos y organizativos (ISSN: 0213-0750), pp. 45-71.

## 7.2. Citas de Internet.

Agencia Española Protección de Datos (España) Tecnologías y Protección de Datos en las AA.PP. [en línea]. ASTIC, Delegado de Protección de Datos del Parlamento de Andalucía, Junta Electoral de Andalucía y Defensor del Pueblo Andaluz, D. Iñaki González-Pol y Dña. Sara Degli Esposti, investigadora del Instituto de Políticas y Bienes Públicos del

CSIC. [Madrid, 19 de noviembre de 2020]: Notas de prensa. <https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-publica-guia-nuevas-tecnologias-aapp>, login: 'aepd' [Consulta: 31 mar. 2021]

Condiciones de uso de Radar Covid (2021), véase https://radarcovid.gob.es/condiciones-de-uso [Última visualización: 24/06/2021]

ISO / IEC 20546: 2019 Tecnología de la información - Big data - Resumen y vocabulario [2019-02] <https://www.iso.org/obp/ui/#iso:std:iso-iec:20546:ed-1:v1:en> login: 'ISO' [Consulta: 31 mar. 2021]

### 7.3. Libros.

APARICIO SALON, Javier. *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal.* Citer Menor, Navarra: Aranzadi, 2009. Ed. 3ª, pp. 369.

LLÁCER MATACÁS, María Rosa. *La autorización al tratamiento de información personal en la contratación de bienes y servicios*. España: Dykinson, 2012., pp. 188.

PÉREZ LUÑO, Antonio-Enríquez. *Nuevas tecnologi□as, sociedad y derecho: el impacto socio-juri□dico de las N. T. de la informacio□n.* Colección Impactos, 1ª E., Madrid, Fundesco, 1987, pp. 154.

### 7.4. Jurisprudencia.

STS 141/2020, Sala Segunda, de lo Penal, de 13 de mayo 2020, RJ 2020/1150, Rec. 2749/2018.

STS 163/2021, Sala Cuarta, de lo Social, de 8 de febrero de 2021, RJ 2021/672, Rec. 84/2019.

STS 766/2020, Sala Cuarta, de lo Social, de 15 de septiembre de 2020, RJ 2020/4005, Rec. 528/2018.

SAN 13/2019, de 6 de febrero de 2019, AS 2019/905, Proc. 318/2018.

SAP 126/2019, de 30 de julio de 2019, JUR 2019/341579, Rec. 193/2019.

### 7.5. Legislación.

Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales https://boe.es/buscar/act.php?id=BOE-A-2018-16673&tn=2

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal https://boe.es/buscar/act.php?id=BOE-A-2008-979

Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil https://boe.es/buscar/act.php?id=BOE-A-1889-4763

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444

Constitución española «BOE» núm. 311, de 29 de diciembre de 1978 https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229

Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores https://www.boe.es/buscar/act.php?id=BOE-A-2015-11430

Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica https://www.boe.es/buscar/doc.php?id=BOE-A-2010-1330