Universidad de Valladolid

icava
Ilustre Colegio de Abogados de Valladolid

Facultad de **Derecho**

Máster de Acceso a la Abogacía

PROTECCIÓN JURISDICCIONAL FRENTE A LA CESIÓN INCONSENTIDA DE DATOS.

Un caso concreto de Facebook

Trabajo realizado por:

Rodrigo Rubia Gómez

Trabajo tutorado por:

Begoña Vidal Fernández

Valladolid, enero de 2021

A ti.

ÍNDICE

HECHOS

Al presente caso, del cual se procede a realizar un dictamen fundamentado normativa y jurisprudencialmente, le son de aplicación los siguientes hechos:

1. D. Daniel Pérez Lobo, mayor de edad, natural de Ávila, tiene como entretenimiento y principal hobby la realización de toda clase de deportes, sobre todo de aventura, los viajes en los que se pueden realizar distintos tipos de actividades deportivas, así como la lectura y la escritura. D. Daniel siempre tiene cuidado de no aportar sus datos personales en establecimientos, comercios electrónicos, uso de banca electrónica, así como otras aplicaciones que requieren de estos, puesto que es muy celoso de su intimidad y no desea que sus datos sean conocidos.
2. Con fecha 2 de marzo de 2019, D. Daniel decide comenzar a relatar todos los viajes, hechos deportivos y actividades de entretenimiento que realiza en una página de Facebook que crea a tal efecto. Al crear esta página de Facebook aporta una serie de datos personales que son exigibles por dicha red social para que pueda iniciar a publicar toda la información que D. Daniel considera relevante y de interés para su público.
3. Con fecha 5 de marzo de 2019 y hasta la actualidad, D. Daniel comienza a recibir una serie de llamadas a su teléfono móvil en un horario que oscila entre las 15:30 y las 18:30, siendo todas estas llamadas realizadas por empresas de teleoperadores que le ofrecen distintos servicios y productos para que proceda a su adquisición; entre ellas destacan las llamadas de empresas de telefonía móvil, seguros, productos financieros, así como de empresas especializadas en los deportes y hobbies que D. Daniel realiza.
4. Durante este periodo de tiempo desde que D. Daniel decide crear la página de Facebook hasta la actualidad, D. Daniel ha estado apuntando todos los sitios donde ha facilitado sus datos personales y ha llegado a la conclusión de que únicamente ha sido en la creación de la página de Facebook en la que relata todos los viajes, hechos deportivos y actividades de entretenimiento que realiza.
5. Con fecha 27 de octubre de 2020, D. Daniel acude al despacho para que se le dé una solución, dada la incomodidad de dichas llamadas recibidas y la cesión que se ha realizado de sus datos personales, por lo que desea que se le elabore un informe fundamentado normativa y jurisprudencialmente al respecto de su caso para conocer

qué puede hacer, dónde puede reclamar y sobre todo contra quién ha de dirigir sus peticiones.

CUESTIONES PLANTEADAS

En relación con los hechos anteriormente expuestos se plantean por D. Daniel una serie de cuestiones jurídicas:

1. ¿Ante qué organismo u organismos puede acudir para defender sus intereses?
2. ¿Puede iniciar un pleito en defensa de sus intereses?
3. ¿Ante qué tribunal o juez y dónde puede presentar un pleito en defensa de sus intereses al tratarse de una empresa multinacional?
4. ¿Qué tipo de proceso será el pleito en defensa de sus intereses?
5. ¿Contra quién debe dirigir sus peticiones?
6. ¿Qué puede reclamar?
7. ¿Sobre qué base jurídica o fundamentación puede reclamar?

NORMATIVA APLICABLE

Normativa Europea:

- Tratado de Funcionamiento de la Unión Europea.
- Carta de los Derechos Fundamentales de la Unión Europea.
- 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.
- Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.
- Guía 03/2019 del Comité Europeo de Protección de Datos.

Normativa española:

- Constitución Española de 1978.
- Ley Orgánica 1/1982 de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.
- Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos, por exigencia de la Disposición Transitoria 4ª de la LOPD.
- Ley Orgánica 3/2018, de 5 diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa.
- Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal.
- Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil.
- Acuerdo de 15 de septiembre de 2005, del Pleno del Consejo General del Poder Judicial, por el que se aprueba el Reglamento 1/2005, de los aspectos accesorios de las actuaciones judiciales.
- Dictamen 5/2009 de 12 de junio de 2009, referente a las redes sociales en línea de la Agencia Española de Protección de Datos.
- Dictamen 0197/2013 de la Agencia Española de Protección de Datos.
- Dictamen del Grupo de Trabajo de la Agencia Española de Protección de Datos, de 12 de junio de 2009, referente a las redes sociales.

FUNDAMENTOS JURÍDICOS

PRIMERO.-

Los datos personales son elementos integrantes del derecho fundamental a la intimidad. La protección de los datos personales es un derecho que tenemos en virtud de lo dispuesto en la distinta normativa referente a ello, y por ende se trata de un derecho por el que todo ciudadano puede disponer de sus datos personales decidiendo de qué manera un tercero puede tratarlos y utilizarlos, así como los fines para los que se utilicen y la duración del uso de los mismos[1].

De tal modo es recogido por el art. 18.4 de la Constitución Española, vinculado a su vez con el art. 18.1 del mismo texto legal, en tanto en cuanto se trata de una manifestación del derecho a la intimidad personal:

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. […]

4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

De igual modo, el derecho de la Unión Europea[2] recoge también este derecho a la protección de los datos personales de los ciudadanos comunitarios en dos de sus principales textos con rango constitucional, como son el Tratado de Funcionamiento de la Unión Europea (TFUE), en su art. 16, así como en la Carta de los Derechos Fundamentales de la Unión Europea (CDFUE), en su art. 8, los cuales se reproducen a continuación:

Art. 16.1 TFUE: Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

Art. 8 CDFUE: 1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

[1] Álvarez Hernando, J (2019). *Protección de datos personales en el proceso.*

[2] Ramiro, M. A. (2005*). El derecho fundamental a la protección de datos personales en Europa.*

Antes de concretar esta normativa en el caso de D. Daniel, es necesario conocer que existe una figura esencial en todo lo relacionado con el tratamiento de los datos personales, incluido en el ámbito de las redes sociales, que es el *responsable del tratamiento de los datos*, el cual será el encargado de velar porque los datos personales de cualquier interesado sean correctamente tratados y gestionados tal y como dispone el art. 24.1 del 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), en adelante RGPD, y que indica lo siguiente:

Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

De igual modo, tienen que ser respetados los distintos derechos que el propio interesado tiene al respecto de sus datos personales, y los cuales aparecen reflejados en el Capítulo III del RGPD, concretamente en los arts. 15 a 18 del texto legal antes nombrado.

- Derecho de acceso del interesado (art. 15 RGPD): Tal y como se dispone en dicho artículo, el interesado, es decir, quien presta sus datos personales, tiene derecho a obtener del responsable de tratamiento una confirmación para saber si sus datos se están tratando del modo correcto o no, de igual modo ha de conocer los fines para los que se están tratando sus datos personales, las categorías de los datos tratados, los destinatarios de sus datos personales, el plazo durante el cual se van a conservar sus datos personales, la existencia del derecho para solicitar al responsable de tratamiento una rectificación, supresión, limitación u oposición para el uso de sus datos personales, el derecho a presentar una reclamación ante una autoridad de control… Siempre que los datos personales del interesado sean transferidos a un tercer país u organización internacional, el interesado tiene derecho a ser informado de las garantías que para ello prevé el art. 46 RGPD. De igual modo, el responsable del tratamiento deberá facilitar una copia de los datos personales que serán objeto de tratamiento sin afectar negativamente a los derechos y libertades de terceros por emitir la copia solicitada por el propio interesado.

- Derecho de rectificación (art. 16 RGPD): De tal como como se dispone en dicho artículo del RGPD, *El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.*
- Derecho de supresión (art. 17 RGPD): Los datos de cualquier interesado deben ser eliminados cuando no cumplan la función para la que fueron recabados, el interesado retire el consentimiento, se oponga al tratamiento de los mismos, dichos datos hayan sido tratados de modo ilícito, deban ser suprimidos para cumplir la legislación procedente o cuando hayan sido hechos públicos.
- Derecho a la limitación del tratamiento (art. 18 RGPD): El interesado tiene derecho a limitar el tratamiento de sus datos cuando se impugne la exactitud de los datos personales hasta verificar los mismos, el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales solicitando la limitación del uso, el responsable del tratamiento no necesite los datos para los fines para los cuales se obtuvieron, o el interesado se oponga al tratamiento hasta que se compruebe si los motivos legítimos del responsable de tratamiento prevalecen sobre los del interesado. Siempre que el interesado limite el uso de sus datos, sus datos personales solo podrán ser objeto de tratamiento por razones de interés público.

Analizados los derechos que tiene en interesado, en este caso D. Daniel, podemos observar que se ha producido una vulneración clara de lo dispuesto en el apartado de Derechos del Interesado del RGPD, dado que se observa una ilicitud en el uso que se está dando a estos datos, puesto que se están entregando a terceros, en este caso a empresas de teleoperadores que le ofrecen distintos servicios y productos para que proceda a su adquisición, empresas de telefonía móvil, seguros, productos financieros, así como de empresas especializadas en los deportes y hobbies que D. Daniel realiza, lo cual demuestra que no se ha informado a D. Daniel de a quién van a ser comunicados sus datos personales, lo que vulnera el art. 15.1.c RGPD.

Tal y como se desprende de la lectura del caso de D. Daniel, al haber creado él mismo el perfil de Facebook[3] para su uso personal, se puede extrapolar que los datos personales que ha aportado han sido indicados directamente por D. Daniel, por lo que los datos personales

[3] Roa Navarrete, M. A. (2013). *Facebook frente al derecho a la vida privada y la protección de datos personales.*

han sido obtenidos directamente del interesado, siéndole de aplicación directa lo establecido en el art. 13 RGPD, por el que se indican cuáles son los datos que deben ser facilitados por el responsable de tratamiento, asunto que sí se cumple en el caso de Facebook[4] dado que en su Política de Datos[5] sí que se indica quién es el responsable de tratamiento de los datos y cómo se puede contactar directamente con él.

En relación con el caso de D. Daniel, tal y como dispone el art. 3.d de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD), así como en el art. 24 del Reglamento de Protección de Datos Personales (en adelante RGPDP), debe existir un responsable de tratamiento de datos personales que debe aplicar las medidas técnicas y organizativas apropiadas con el fin de garantizar que el tratamiento de los datos personales del interesado se realiza tal y como dispone el Reglamento antes citado.

En España se cuenta con un órgano que ejerce a su vez funciones de vigilancia en cuanto al tratamiento de datos personales se refiere, como igualmente de redacción de dictámenes jurídicos al respecto de todo ello, este órgano es la Agencia Española de Protección de Datos (en adelante AEPD), en cuyo Dictamen 5/2009 de 12 de junio de 2009, referente a las redes sociales en línea, establece que en virtud del art. 29 de la Directiva 95/46/CE, los proveedores de servicios de redes sociales son responsables del tratamiento de los datos personales de sus usuarios dado que han de proporcionar todos los medios para permitir que el tratamiento de los datos de usuarios sea el correcto, así como los servicios vinculados a la gestión de los usuarios referentes al registro y supresión de cuentas entre otros.

De igual modo, en dicho Dictamen 5/2009 AEPD, se señala que los usuarios, para poder crear un perfil en las redes sociales han de aportar una serie de datos personales para poder generar su propio perfil o página de interés. Es por este motivo que la red social, en este caso Facebook, está realizando un tratamiento de datos personales tal y como se describe en los arts. 24 y 28 RGPD, así como en el art. 5.1.t LOPD por el que se explicita que desde el momento en que un usuario proporciona una serie de datos personales ya se está procediendo a una operación que inicia una relación en el tratamiento de los datos personales.

[4] Díaz, E. D. (2018). *Protección de datos: lecciones del caso Facebook. Nuestro tiempo.*

[5] Facebook

La AEPD considera que la relación entre un usuario de redes sociales y la propia red social[6] se inicia desde el momento en que existe un consentimiento libre por aquel que cede sus datos personales y el receptor los acepta, siempre y cuando no exista un vicio en dicho consentimiento a la luz de lo dispuesto en el art. 1262 del Código Civil en relación con el art. 7 RGPD referente a las condiciones para que exista un consentimiento. Siendo en este caso un consentimiento referente a una operación por la cual se procede al tratamiento de una serie de datos personales con un fin determinado, legítimo y correctamente explicitado, la AEPD[7] considera que el consentimiento inequívoco se da en el momento en que se *exige la realización de una acción u omisión que implique la existencia de consentimiento*.

El usuario de las redes sociales debe conocer en todo momento la información referente a sus datos personales y cómo va a ser tratada por la red social, por lo que para ello le será de aplicación lo dispuesto y anteriormente explicado en el art. 13 RGPD, es por ello que siempre y antes de que se realice el registro del usuario en las redes sociales, el proveedor de las redes sociales ha de aportar una información clara y completa referente a los fines y modos en que sus datos personales van a ser tratados. En consecuencia, el citado Dictamen 5/2009 AEPD, señala lo siguiente:

Los proveedores de SRS deberían informar a los usuarios de su identidad y de los distintos fines para los que tratan los datos personales, de conformidad con las disposiciones del artículo 10 de la Directiva relativa a la protección de datos, a saber, entre otras cosas:

- la utilización de los datos con fines de comercialización directa;

- la posible distribución de datos a categorías específicas de terceros;

- una reseña de los perfiles: su creación y sus principales fuentes de datos;

- la utilización de datos sensibles

Por todo ello y como resumen de lo anteriormente expuesto, para que una cesión de datos personales de un usuario a un proveedor de servicio de redes sociales sea válida será necesario que exista un consentimiento expreso, válido y no viciado tal y como se dispone en el Código Civil, de igual modo, en el caso de que se traten datos personales referentes a la raza, salud y

[6] Agencia Española de Protección de Datos. *Informe sobre el interés legítimo en la protección de datos de carácter personal.*

[7] Agencia Española de Protección de Datos. *Informe 210070/2018*.

orientación sexual el consentimiento será expreso, si además se hace referencia a la ideología, afiliación sindical, religión o creencias deberá ser por escrito. En relación con el deber de información se estará a lo dispuesto en la Sentencia del Tribunal Supremo de 15 de julio de 2010 (Rec. 23/2008) en virtud del efecto producido por dicha sentencia, dejando nulos y sin efectos los artículos 11, 18, 38.2, y 123.2 de la disposición reglamentaria, así como la frase del artículo 38.1.a) que dice así: "... y al respecto de la cual no se haya entablado reclamación judicial, arbitral o administrativa, o tratándose de servicios financieros, no se haya planteado una reclamación en los términos previstos en el reglamento de los Comisionados para la defensa del cliente de servicios financieros, aprobado por Real Decreto 303/2004, de 20 de febrero" del 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..

Cuando los datos personales hayan sido recabados de manera online, la AEPD[8] considera que el deber de información por parte del proveedor de redes sociales se ve completado desde el momento en que existe una política de privacidad de datos accesible y fácil de entender, considerándose prueba suficiente que para poder introducir los datos y darse de alta en la red social se han debido de aceptar las políticas de datos de la red social, por lo que el fin para el que se utilicen los datos personales recabados por la red social han de estar claramente descritos y especificados en la Política de Datos de la red social, considerándose esto prueba suficiente de quedar acreditado el deber de información.

Según el propio Dictamen 0197/2013 AEPD, desde el momento en el que cualquier material audiovisual que un usuario (persona física), como es el caso de D. Daniel, sube a cualquier plataforma que preste el servicio de redes sociales se considera dato personal, de igual modo tal y como el RGPD dispone y se ha especificado anteriormente, es el responsable del fichero, y por tanto el responsable del tratamiento, quien debe adoptar las medidas técnicas y organizativas para que la seguridad de los datos de carácter personal, su alteración, pérdida, tratamiento o acceso no autorizado sean debidamente seguros y se garantice que no se hace de los mismos un uso ilícito, en tanto en cuanto su almacenamiento, y por ende la exposición de los mismos a terceros ajenos a los mismos, son derivados de las acciones que el propio fichero tiene por el mero hecho de ser un fichero. Para ello, el propio responsable de tratamiento de los datos personales habrá de establecer una serie de criterios y parámetros

[8] Agencia Española de Protección de Datos. *Informe 0197/2013*.

relativos a la confidencialidad de dichos datos que sean publicados en el perfil que el usuario tiene en la red social, por lo que ante el hecho de carecer de parámetros de confidencialidad válidos y claros, cualquier tercero podrá hacer uso de los datos que el propio usuario tenga depositados en la red social, por lo que los parámetros establecidos por defecto han de ser garantes de la privacidad y la intimidad personal.

SEGUNDO.-

Procede hacer con carácter preliminar un breve análisis en lo referente a las redes sociales y a lo que disponen los arts. 2 y 18 RGPD. En el primero se indica que *"El presente Reglamento no se aplica al tratamiento de datos de carácter personal por una persona física en el curso de una actividad exclusivamente personal o doméstica y, por tanto, sin conexión alguna con una actividad profesional o comercial"*, mientras que en el art. 18 del anterior cuerpo legal se especifica claramente que *"Las actividades personales y domésticas incluyen la correspondencia y llevanza de un repertorio de direcciones, la actividad en redes sociales y la actividad en línea realizada en el contexto de las anteriores actividades citadas"*. Por lo que surge la duda de si lo que D. Daniel está haciendo en su perfil de Facebook es una actividad doméstica que queda desprotegida o no lo es.

Para ello será necesario analizar previamente una serie de documentos que permitirán determinar si la actividad de D. Daniel es considerada actividad doméstica o si por el contrario excede ese ámbito personal y doméstico.

1. En primer lugar es necesario acudir a la jurisprudencia española con un análisis de la Sentencia de la Audiencia Nacional, Sala de lo Contencioso, Sección 1, de 11 de mayo de 2018[9], referente a un caso en el cual un vídeo de una vista de juicio oral es publicada en Facebook, por lo que la Audiencia Nacional decide aplicar lo dispuesto en el Dictamen del Grupo de Trabajo, de 12 de junio de 2009, referente a las redes sociales, el cual hace una referencia expresa a qué es una actividad doméstica de redes sociales, que es la habitual por la mayoría de los usuarios, y cuál es la actividad protegida por el RGPD. Igualmente, las sentencias de la Audiencia Nacional, Sala de lo Contencioso, de 27 de diciembre de 2019[10], y de 30 de octubre de 2020[11] demuestran el modo en que la Audiencia Nacional actúa frente a la intromisión de las empresas en los datos personales de los usuarios de las mismas. En este segundo caso, se está a lo dispuesto por el propio Grupo de Trabajo en base a tres supuestos que exceden el uso doméstico:

[9] SAN 2264/2018, ECLI: ES:AN:2018:2264

[10] SAN 5188/2018, ECLI: ES:AN:2019:5188.

[11] SAN 3182/2020, ECLI: ES:AN:2020:3182.

a. Cuando las redes sociales son utilizadas como una plataforma para hallar soluciones empresariales o que den respuesta a los usos y haceres de una asociación.
b. Cuando el acceso a la información que existe en el perfil presente en las redes sociales excede los contactos seleccionados por el usuario o cuando los datos de dicho perfil en redes sociales son indexables por los motores de búsqueda habituales.
c. Cuando los datos que contiene dicho perfil son sensibles tal y como los cataloga el propio RGPD (raza o etnia, opiniones políticas, creencias religiosas o filosóficas, pertenencia a un sindicato, orientación sexual, datos de salud…).

2. En segundo lugar, es necesario acudir a las guías establecidas por el Comité Europeo de Protección de Datos, en concreto a la Guía 03/2019, la cual establece que, tal y como en repetidas ocasiones ha establecido el TJUE, la exención del hogar únicamente puede interpretarse como en aquellas actividades que se realizan en el curso de la vida familiar o privada, lo cual se contradice con el acceso a infinidad de usuarios de los datos personales presentes en las redes sociales.
3. En tercer y último lugar, es conveniente analizar la sentencia Lindqvist del Tribunal de Justicia de la Unión Europea (C101/01)[12], de 6 de noviembre de 2003, en la cual se sientan las bases y sirve de apoyo natural a las guías del Comité Europeo de Protección de Datos, en cuyo fallo, el propio Tribunal establece que la exención del hogar únicamente es aplicable cuando las actividades que sean publicadas en las redes sociales sean referentes a la vida familiar y privada, y el acceso a las mismas sea a un grupo discriminado de personas establecidas por el usuario y no la infinitud de personas que pueden acceder a cualquier dato público actualmente en manos de las redes sociales.

Por todo ello podemos concluir que la actividad que D. Daniel realiza no es de las consideradas como ámbito doméstico, puesto que haciendo una búsqueda básica en Google se puede obtener la información relativa al perfil de Facebook de D. Daniel Pérez Lobo como se puede ver en la imagen inferior:

[12] ECLI:EU:C:2003:596

Es por ello por lo que ya se está incumpliendo el requisito de la Sentencia de la Audiencia Nacional antes analizada, puesto que los datos de D. Daniel son, por tanto, indexables y se pueden localizar mediante el uso de un motor de búsqueda, por lo que ya exceden del uso doméstico que se le puede dar a una red social, lo que convierte las pretensiones de D. Daniel en plenamente viables y dan pie a que pueda actuar en beneficio de sus intereses.

Cualquier usuario de redes sociales podrá defender sus intereses por el simple hecho de ser usuario de estas ante distintos órganos:

- El primer paso es contactar con el responsable del tratamiento de las redes sociales concretas, en este caso de Facebook, para poder ejercitar su derecho de acceso, rectificación, limitación, oposición, supresión, portabilidad y oposición al tratamiento de decisiones automatizadas. En el caso concreto de D. Daniel, al ser usuario de Facebook, deberá ejercitar sus derechos ante el responsable de Tratamiento de Facebook, lo cual es accesible mediante el siguiente enlace de la propia página de Facebook, el cual remite a la política de datos y privacidad de la red social, y que propone a interés de los afectados el contacto mediante una dirección física:

  Facebook Ireland Ltd.
  4 Grand Canal Square
  Grand Canal Harbour
  Dublín 2 Irlanda

  Además, Facebook indica en dicho enlace, que es posible, como usuario, ejercer el derecho de presentar una reclamación ante la autoridad de control principal de

Facebook Ireland, en concreto a la Comisión de Protección de Datos de Irlanda, o en su defecto a la autoridad de control local.

- En segundo lugar, se puede elegir presentar una reclamación ante la Comisión de Protección de Datos de Irlanda, cosa que no se debe recomendar a D. Daniel puesto que la legislación irlandesa es bastante más laxa en ese contexto de defensa de los consumidores y usuarios, motivo por el cual la mayoría de las empresas tecnológicas tienen su sede europea en dicho territorio, y no solo por los beneficios fiscales como es comúnmente conocido; o bien presentarla en el organismo local competente, en este caso ante la Agencia Española de Protección de Datos.

  En el segundo caso concreto, que es el que se recomienda para D. Daniel, lo esencial es presentar, en primer lugar, una acreditación de que se han ejercido los derechos al acceso, rectificación, limitación, oposición, supresión, portabilidad y oposición al tratamiento de decisiones automatizadas ante el responsable de tratamiento de datos de Facebook. En el momento en que eso pueda ser probado y se considere que ha pasado un plazo suficiente sin que se haya recibido respuesta o que la respuesta recibida es inadecuada, se puede interponer una reclamación ante la AEPD, ante la cual se deberán aportar documentos o pruebas que verifiquen que la red social correspondiente está cometiendo una infracción de la normativa de protección de datos personales del usuario. En caso de que la AEPD no se considere competente para realizar los trámites relativos a dicha reclamación, o su análisis derive en que existen otras vías tangentes de carácter judicial (vía civil y penal) que pueden resolverlo de un modo más claro y efectivo, será la propia AEPD la que indicará al reclamante cómo debe actuar y cuáles son los pasos a seguir. Igualmente, en caso de que la reclamación planteada sea competencia de las autoridades autonómicas de protección de datos, será la propia AEPD la que realizará la comunicación y tramitará todo lo relativo a dicha reclamación con las propias administraciones autonómicas para que sean ellas las que resuelvan en consecuencia.

- En tercer lugar, pero no menos importante, destaca el papel de las Asociaciones y Organizaciones de Consumidores y Usuarios, y en este caso el papel de la OCU es fundamental. Estas Asociaciones tienen la legitimación prevista en el art. 11 de la Ley de Enjuiciamiento Civil para actuar procesalmente en defensa de los consumidores y usuarios, lo que ya ha sucedido al haber presentado la OCU una demanda colectiva contra Facebook y WhatsApp (siendo WhatsApp actualmente propiedad de Facebook) como derivación natural del escándalo producido por el caso Cambridge

Analytica, momento en el cual se hace público y evidente que Facebook, tras recopilar los datos de los usuarios, procede a utilizarlos sin consentimiento expreso de los mismos, lo que vulnera claramente la normativa relativa a la Protección de Datos de Carácter Personal.

- En cuarto lugar, se sitúa el sistema jurisdiccional español, ante cuyos tribunales se puede presentar una demanda o denuncia, dependiendo de si lo reclamado lo es en la vía civil o en la vía penal[13], respectivamente. Como en este caso concreto D. Daniel puede actuar por ambas vías se va a proceder al análisis concreto de cada una de ellas, las condiciones que se han de dar y lo que se puede reclamar en ambas.

[13] Sentencia del Tribunal Supremo de 13 de abril de 2009, ECLI: ES:TS:2009:3015 y Sentencia del Tribunal Supremo de 29 de abril de 2019, ECLI: ES:TS:2019:1383.

TERCERO.-

¿Puede iniciar un pleito en defensa de sus intereses? Ante qué tribunal o juez y dónde, pues se trata de una empresa multinacional, y qué tipo de proceso sería.

D. Daniel sí que puede iniciar un pleito en defensa de sus intereses, dado que, en virtud de lo explicado en el apartado anterior, D. Daniel no hace un uso doméstico de sus redes sociales, en este caso de la página de Facebook, puesto que se incumple desde el primer momento uno de los requisitos que expone la Sentencia de la Audiencia Nacional, Sala de lo Contencioso, de 11 de mayo de 2018[14], para que sea considerado un uso doméstico de las redes sociales. Los datos de D. Daniel son indexables y se pueden localizar mediante el uso de un motor de búsqueda, por lo que ya exceden del uso doméstico que se le puede dar a una red social, lo que convierte las pretensiones de D. Daniel en plenamente viables y le legitiman para que pueda actuar en defensa de sus intereses.

Como se ha explicado anteriormente, D. Daniel puede iniciar el camino mediante una reclamación a Facebook de modo directo, contactando con el responsable de tratamiento en la dirección antes indicada, siendo éste el paso primordial y esencial como condición previa a un procedimiento judicial. Una vez que D. Daniel haya realizado la reclamación ejercitando sus derechos al acceso, rectificación, limitación, oposición, supresión, portabilidad u oposición al tratamiento de decisiones automatizadas ante el responsable de tratamiento de datos de Facebook, puede continuar mediante la interposición de la reclamación ante la AEPD si lo desea, actuación que dará lugar a que sea la propia la AEPD la que considere si ella misma es competente para tramitar y realizar todos los pasos necesarios para que dicha reclamación sea hecha efectiva, para ello necesitará de la aportación de pruebas y documentos que demuestren que la red social está realizando algún tipo de uso ilegítimo de sus datos personales, en este caso concreto se recomienda acreditación de las llamadas, grabación de las mismas, aportación de correos electrónicos de publicidad si los hubiera recibido, etc.

Si bien esta es una vía que D. Daniel puede tomar, la pregunta estricta es cómo puede iniciar el pleito en defensa de sus intereses, para ello es recomendable que D. Daniel comience su reclamación en la vía civil y realizar una reclamación estrictamente económica de los daños y perjuicios causados, reservándose la posibilidad de actuar penalmente, para, una vez visto el resultado del procedimiento civil, acudir a la jurisdicción penal.

[14] SAN 2264/2018, ECLI: ES:AN:2018:2264

Otra posibilidad es la actuación en vía contencioso-administrativa, que se expone a continuación.

- En relación con el proceso contencioso administrativo se recomienda a D. Daniel que previamente denuncie los hechos ante la AEPD indicando lo anteriormente expuesto. Dependiendo de la resolución que la AEPD emita en este caso determinado se pueden establecer tres vías.
    - La primera de ellas surge si la propia AEPD considera que se han violado y cedido sin consentimiento los propios datos personales de D. Daniel, en cuyo caso será la propia AEPD la que inicie el procedimiento contra Facebook para determinar una retrocesión a la situación inicial, eliminar el mal causado y en un hipotético caso llegar a una compensación económica a D. Daniel, siendo la propia AEPD la que realice todo el procedimiento sin necesidad de intervención del propio perjudicado.
    - La segunda aparece en caso de que la AEPD no se considere competente para tramitar el asunto, en cuyo caso aportará a D. Daniel toda la información necesaria para que inicie las acciones judiciales necesarias por su cuenta para poder solventar el asunto y reinstaurar sus derechos que la propia LOPD y RGPD le atribuyen como usuario de las redes sociales. En ese momento la AEPD desaparece y se produce un posible inicio por vía de recurso contra esta resolución tal y como se relatará en el siguiente punto.
    - La tercera se establece cuando la AEPD dicta una resolución no adecuada a los intereses del perjudicado, bien por ausencia de motivación, falta de forma o fondo o por causas ajenas al hecho en cuestión. Contra esta resolución caben dos recursos de naturaleza administrativa, susceptibles de agotar la vía administrativa.

- Recurso de reposición que se habrá de interponer ante el propio Director de la AEPD y que se regula en los arts. 123[15] y 124[16] de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en los cuales se establece que el recurso de reposición se ha de interponer ante el mismo organismo que hubiera dictado la resolución, y ante su desestimación cabrá interponer recurso contencioso administrativo. El plazo para interponer este recurso es de un mes desde la notificación del acto administrativo que se pretende recurrir. Por su parte la AEPD dispone de un mes para resolver dicho recurso y contra dicha resolución, que agota la vía administrativa, únicamente cabe recurso contencioso-administrativo.
- Recurso extraordinario de revisión, que se habrá de interponer ante la misma AEPD siempre y cuando concurran las circunstancias previstas en el art. 125[17] de la Ley 39/2015, en el plazo de cuatro años

[15] **Artículo 123**. Objeto y naturaleza.

1. Los actos administrativos que pongan fin a la vía administrativa podrán ser recurridos potestativamente en reposición ante el mismo órgano que los hubiera dictado o ser impugnados directamente ante el orden jurisdiccional contencioso-administrativo.

2. No se podrá interponer recurso contencioso-administrativo hasta que sea resuelto expresamente o se haya producido la desestimación presunta del recurso de reposición interpuesto.

[16] **Artículo 124**. Plazos.

1. El plazo para la interposición del recurso de reposición será de un mes, si el acto fuera expreso. Transcurrido dicho plazo, únicamente podrá interponerse recurso contencioso-administrativo, sin perjuicio, en su caso, de la procedencia del recurso extraordinario de revisión. Si el acto no fuera expreso, el solicitante y otros posibles interesados podrán interponer recurso de reposición en cualquier momento a partir del día siguiente a aquel en que, de acuerdo con su normativa específica, se produzca el acto presunto.

2. El plazo máximo para dictar y notificar la resolución del recurso será de un mes.

3. Contra la resolución de un recurso de reposición no podrá interponerse de nuevo dicho recurso.

[17] **Artículo 125**. Objeto y plazos.

1. Contra los actos firmes en vía administrativa podrá interponerse el recurso extraordinario de revisión ante el órgano administrativo que los dictó, que también será el competente para su resolución, cuando concurra alguna de las circunstancias siguientes:

-para lo establecido en el art. 125.1.a de dicho texto legal- o de tres meses, desde que se tenga conocimiento de la existencia de los documentos o desde que la sentencia judicial devenga firme en el caso de los arts. 125.1.b, c y d del mismo texto legal. Dicho recurso se habrá de resolver en un plazo de tres meses, o mediante silencio administrativo desestimatorio en el mismo plazo, tal y como dispone el art. 126[18] de la Ley 39/2015.

---

a) Que al dictarlos se hubiera incurrido en error de hecho, que resulte de los propios documentos incorporados al expediente.

b) Que aparezcan documentos de valor esencial para la resolución del asunto que, aunque sean posteriores, evidencien el error de la resolución recurrida.

c) Que en la resolución hayan influido esencialmente documentos o testimonios declarados falsos por sentencia judicial firme, anterior o posterior a aquella resolución.

d) Que la resolución se hubiese dictado como consecuencia de prevaricación, cohecho, violencia, maquinación fraudulenta u otra conducta punible y se haya declarado así en virtud de sentencia judicial firme.

2. El recurso extraordinario de revisión se interpondrá, cuando se trate de la causa a) del apartado anterior, dentro del plazo de cuatro años siguientes a la fecha de la notificación de la resolución impugnada. En los demás casos, el plazo será de tres meses a contar desde el conocimiento de los documentos o desde que la sentencia judicial quedó firme.

3. Lo establecido en el presente artículo no perjudica el derecho de los interesados a formular la solicitud y la instancia a que se refieren los artículos 106 y 109.2 de la presente Ley ni su derecho a que las mismas se sustancien y resuelvan.

[18] **Artículo 126.** Resolución.

1. El órgano competente para la resolución del recurso podrá acordar motivadamente la inadmisión a trámite, sin necesidad de recabar dictamen del Consejo de Estado u órgano consultivo de la Comunidad Autónoma, cuando el mismo no se funde en alguna de las causas previstas en el apartado 1 del artículo anterior o en el supuesto de que se hubiesen desestimado en cuanto al fondo otros recursos sustancialmente iguales.

2. El órgano al que corresponde conocer del recurso extraordinario de revisión debe pronunciarse no sólo sobre la procedencia del recurso, sino también, en su caso, sobre el fondo de la cuestión resuelta por el acto recurrido.

3. Transcurrido el plazo de tres meses desde la interposición del recurso extraordinario de revisión sin haberse dictado y notificado la resolución, se entenderá desestimado, quedando expedita la vía jurisdiccional contencioso-administrativa.

- Una vez agotada la vía administrativa cabe pasar a la judicial presentando un recurso contencioso-administrativo se puede interponer tras los plazos y resoluciones de los recursos anteriormente expuestos. En este caso se ha de interponer ante la Sala de lo Contencioso-Administrativo de la Audiencia Nacional tal y como establece la disposición adicional cuarta en su apartado quinto[19], así como los arts. 25[20], 46[21] de

[19] **Disposición adicional cuarta. Recursos contra determinados actos, resoluciones y disposiciones.**

Serán recurribles: […] Los actos y disposiciones dictados por la Agencia Española de Protección de Datos, Comisión Nacional de los Mercados y la Competencia, Consejo Económico y Social, Instituto Cervantes, Consejo de Seguridad Nuclear, Consejo de Universidades y Sección Segunda de la Comisión de Propiedad Intelectual, directamente, ante la Sala de lo Contencioso-Administrativo de la Audiencia Nacional.

[20] **Artículo 25.**

1. El recurso contencioso-administrativo es admisible en relación con las disposiciones de carácter general y con los actos expresos y presuntos de la Administración pública que pongan fin a la vía administrativa, ya sean definitivos o de trámite, si estos últimos deciden directa o indirectamente el fondo del asunto, determinan la imposibilidad de continuar el procedimiento, producen indefensión o perjuicio irreparable a derechos o intereses legítimos.

2. También es admisible el recurso contra la inactividad de la Administración y contra sus actuaciones materiales que constituyan vía de hecho, en los términos establecidos en esta Ley.

[21] **Artículo 46.**

1. El plazo para interponer el recurso contencioso-administrativo será de dos meses contados desde el día siguiente al de la publicación de la disposición impugnada o al de la notificación o publicación del acto que ponga fin a la vía administrativa, si fuera expreso. Si no lo fuera, el plazo será de seis meses y se contará, para el solicitante y otros posibles interesados, a partir del día siguiente a aquél en que, de acuerdo con su normativa específica, se produzca el acto presunto.

2. En los supuestos previstos en el artículo 29, los dos meses se contarán a partir del día siguiente al vencimiento de los plazos señalados en dicho artículo.

3. Si el recurso contencioso-administrativo se dirigiera contra una actuación en vía de hecho, el plazo para interponer el recurso será de diez días a contar desde el día siguiente a la terminación del plazo establecido en el artículo 30. Si no hubiere requerimiento, el plazo será de veinte días desde el día en que se inició la actuación administrativa en vía de hecho.

4. El plazo para interponer el recurso contencioso-administrativo se contará desde el día siguiente a aquel en que se notifique la resolución expresa del recurso potestativo de reposición o en que éste deba entenderse presuntamente desestimado.

la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa. En dichos artículos se establece que el plazo para interponer dicho recurso contencioso-administrativo es de dos meses desde el momento en que la AEPD notifica su resolución, o bien transcurridos dos meses desde la resolución del recurso de reposición o del recurso extraordinario de revisión. En el posible escenario de que la AEPD no resolviera el recurso de reposición, se tomará como fecha aquella en la que dicho recurso debiera haber sido resuelto y se tendrá un plazo de seis meses para interponer el recurso contencioso-administrativo tal y como reflejan las sentencias del Tribunal Supremo de 15 de julio de 2010[22] y de 19 de noviembre de 2020[23].

Es importante informar a D. Daniel de que no es necesario seguir toda la escala de los recursos tal y como se ha establecido, sino que el posible acudir directamente al recurso contencioso-administrativo sin pasar previamente por el recurso de reposición, dado que la ley así lo prevé y no es un requisito *sine qua non* para poder al presentar el recurso contencioso-administrativo.

Igualmente, en este caso habrá que valorar la intención última de D. Daniel, puesto que, si su único interés es que se cesen las llamadas y el contacto con su persona por haberse accedido a sus datos personales de modo ilícito, entonces la vía de la AEPD es la ideal para que pueda llegar a lograr su fin. Si por el contrario D. Daniel decide que quiere obtener un beneficio económico y/o una condena para la empresa que ha cedido sus datos, entonces será necesario acudir a la jurisdicción civil y penal respectivamente, en cuyo caso la resolución de la AEPD será un mero trámite para poder establecer la existencia de una reclamación extrajudicial previa.

5. El plazo para interponer recurso de lesividad será de dos meses a contar desde el día siguiente a la fecha de la declaración de lesividad.

6. En los litigios entre Administraciones, el plazo para interponer recurso contencioso-administrativo será de dos meses, salvo que por Ley se establezca otra cosa. Cuando hubiera precedido el requerimiento regulado en los tres primeros apartados del artículo 44, el plazo se contará desde el día siguiente a aquel en que se reciba la comunicación del acuerdo expreso o se entienda presuntamente rechazado.

[22] ECLI:ES:TS:2012:585

[23] ECLI:ES:TS:2020:1562

- En relación con la vía penal, solamente se puede iniciar la vía judicial en presencia de hechos constitutivos de un delito contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio recogidos en el Libro II, Título X del Código Penal, en concreto de una vulneración del art. 197.2 del texto legal anteriormente citado en tanto en cuanto se cumplen los requisitos dispuestos en dicho ilícito penal:
  Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.
  La pena prevista es una pena de privación de libertad de entre uno y cuatro años y una multa de doce a veinticuatro meses al responsable de la cesión de dichos datos por ser *quien, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar que se hallen registrados en ficheros ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado*, cumpliéndose por tanto los elementos del tipo de modo claro.

  Respecto al juzgado competente para conocer de este asunto, se está ante una situación de compleja solución, puesto que, al tratarse de una cesión de datos de carácter personal, y dichos datos estar registrados en los servidores de Facebook en Lulea (Suecia), o en servidores circulantes a nivel mundial del tipo "nube" o servidor cambiante, es difícil establecer dónde se comete el delito de revelación de secretos por el cual se le está encausando, ante esta duda que surge para decidir si se ha de denunciar a Facebook en su sede central o a Facebook en su sede española, es necesario saber dónde se alojan dichos datos, que en este caso es en Lulea (Suecia), en Cloone (Irlanda) o en Dinamarca. Además, es necesario considerar que los datos de todos los usuarios de Facebook no están únicamente almacenados en un único servidor, sino que se encuentran duplicados en los 17 servidores que Facebook tiene en el planeta. Cuando un servidor se "calienta" se ha de pasar a un servidor "frío" para poder hacer uso de esos datos, pero del uso que se da a dichos datos y del tratamiento de los mismos responden, según las propias indicaciones de Facebook (referenciado en webgrafía), las centrales que tienen establecidas en cada uno de los países o sedes nacionales, siendo la propia central de cada uno de los países la que gestiona, trata y hace uso de los datos de los usuarios de la zona geográfica que le sea

de aplicación. En este caso es Facebook Spain[24] la que trata y gestiona los datos de los usuarios españoles.

Sin perjuicio de todo ello conviene analizar la posibilidad de que el delito se hubiera cometido fuera de nuestras fronteras, a lo que le sería de aplicación lo dispuesto en el art. 65 LOPJ, el cual indica que cuando el delito se cometa fuera del territorio nacional y su enjuiciamiento corresponda a los Tribunales españoles, se estará ante una instrucción dependiente de los Juzgados Centrales de Instrucción y de lo Penal, si se parte de la base de que se desconoce el lugar donde dichos datos personales de D. Daniel han sido cedidos se estará ante lo dispuesto en este artículo, iniciándose dicho, siendo el mismo el que tendría que declararse competente, previa explicación de los servidores itinerantes y que la revelación de los datos ha podido ser en cualquier parte del mundo, para que se declare competente para instruir este procedimiento. En su defecto, y subsidiariamente, será el Juzgado de Instrucción que por turno corresponda de Madrid el que deberá conocer de este asunto.

En caso de que se considere que la cesión de datos de D. Daniel ha sido producida por Facebook Spain, opción más clara y viable dado el objeto social que dicha mercantil tiene en España y las labores que desempeña en el tratamiento y uso de los datos personales de los usuarios de dicha red social del territorio geográfico español, se estará ante lo dispuesto en el art. 23.1 LOPJ, puesto que se trata de un delito cometido en el territorio español y por ende ser competente los tribunales españoles para el enjuiciamiento de dicha causa.

Es por ello, que dado que Facebook tiene una sede social en España con el nombre Facebook Spain S.L. sita en Paseo de la Castellana, 35B, 28046, Madrid, que tal y como se puede ver en su objeto social se dedica a la gestión de las redes sociales.
Al existir una sede social en España, tal y como dispone el art. 15 LECRIM[25] será posible interponer la denuncia de un procedimiento ordinario ante los tribunales de

[24] Dumortier, F. (2009). *Facebook y los riesgos de la «descontextualización» de la información*.

[25] **Artículo 15.**

Cuando no conste el lugar en que se haya cometido una falta o delito, serán Jueces y Tribunales competentes en su caso para conocer de la causa o juicio:

1.º El del término municipal, partido o circunscripción en que se hayan descubierto pruebas materiales del delito.

2.º El del término municipal, partido o circunscripción en que el presunto reo haya sido aprehendido.

Madrid, por lo que, en virtud del fuero del "domicilio del presunto reo", en este caso la delegación de Facebook Spain, en tanto en cuanto su objeto social es la gestión de red social en internet, y por ende ser responsables como sede en territorio español de los delitos que pudiera haber cometido la central de Facebook sita en Silicon Valley, se estima que el domicilio del presunto culpable, como representante, es la competencia territorial ante donde se debe iniciar el procedimiento, aunque se promueva contra una persona jurídica en este caso, según lo establecido en el art. 14bis LECRIM[26].

En este caso concreto, es de aplicación lo dispuesto por el art. 119 LECRIM al tratarse de una persona jurídica:

1. Cuando de acuerdo con lo dispuesto en el artículo 118 de esta Ley, haya de procederse a la imputación de una persona jurídica, se practicará con ésta la comparecencia prevista en el artículo 775, con las siguientes particularidades:

a) La citación se hará en el domicilio social de la persona jurídica, requiriendo a la entidad que proceda a la designación de un representante, así como Abogado y Procurador para ese procedimiento, con la advertencia de que, en caso de no hacerlo, se procederá a la designación de oficio de estos dos

3.º El de la residencia del reo presunto.

4.º Cualquiera que hubiese tenido noticia del delito.

Si se suscitase competencia entre estos Jueces o Tribunales, se decidirá dando la preferencia por el orden con que están expresados en los números que preceden.

Tan luego como conste el lugar en que se hubiese cometido el delito, el Juez o Tribunal que estuviere conociendo de la causa acordará la inhibición en favor del competente, poniendo en su caso los detenidos a disposición del mismo y acordando remitir, en la misma resolución las diligencias y efectos ocupados.

[26] **Artículo 14 bis.**

Cuando de acuerdo con lo dispuesto en el artículo anterior el conocimiento y fallo de una causa por delito dependa de la gravedad de la pena señalada a éste por la ley se atenderá en todo caso a la pena legalmente prevista para la persona física, aun cuando el procedimiento se dirija exclusivamente contra una persona jurídica.

últimos. La falta de designación del representante no impedirá la sustanciación del procedimiento con el Abogado y Procurador designado.

b) La comparecencia se practicará con el representante especialmente designado de la persona jurídica imputada acompañada del Abogado de la misma. La inasistencia al acto de dicho representante determinará la práctica del mismo con el Abogado de la entidad.

c) El Juez informará al representante de la persona jurídica imputada o, en su caso, al Abogado, de los hechos que se imputan a ésta. Esta información se facilitará por escrito o mediante entrega de una copia de la denuncia o querella presentada.

d) La designación del Procurador sustituirá a la indicación del domicilio a efectos de notificaciones, practicándose con el Procurador designado todos los actos de comunicación posteriores, incluidos aquellos a los que esta Ley asigna carácter personal. Si el Procurador ha sido nombrado de oficio se comunicará su identidad a la persona jurídica imputada.

También es reseñable, que, al tratarse de una persona jurídica sospechosa, en este caso se puede acoger a lo dispuesto en el art. 409bis del mismo texto legal. Se tomará declaración al representante especialmente designado por la persona jurídica asistido de abogado, en dicha declaración se intentará averiguar la participación de la mercantil, así como las personas que pudieran haber estado implicadas en dicho delito, pudiendo guardar silencio, no declarar contra sí misma y no confesarse culpable. En caso de que no compareciera la persona designada por la persona jurídica se entiende que se acoge a su derecho a no declarar.

En este procedimiento penal lo ideal es que D. Daniel solicite una serie de medidas cautelares acogiéndose a lo dispuesto en el art. 544 quáter LECRIM, entre ellas se le recomendará que solicite que sus datos personales sean borrados de cualquier base de datos a expensas de lo que pueda suceder durante el procedimiento penal.

Como en este caso concreto se está acusando a una persona jurídica, le será de aplicación lo dispuesto en el art. 786 bis LECRIM que se procede a reproducir por establecer con claridad todas las especialidades que esta denunciada puede tener:

1. Cuando el acusado sea una persona jurídica, ésta podrá estar representada para un mejor ejercicio del derecho de defensa por una persona que especialmente designe, debiendo ocupar en la Sala el lugar reservado a los acusados. Dicha persona podrá declarar en nombre de la persona jurídica si se hubiera propuesto y admitido esa prueba, sin perjuicio del derecho a guardar silencio, a no declarar contra sí

mismo y a no confesarse culpable, así como ejercer el derecho a la última palabra al finalizar el acto del juicio.

No se podrá designar a estos efectos a quien haya de declarar en el juicio como testigo.

2. No obstante lo anterior, la incomparecencia de la persona especialmente designada por la persona jurídica para su representación no impedirá en ningún caso la celebración de la vista, que se llevará a cabo con la presencia del Abogado y el Procurador de ésta.

En todo momento las acciones civiles correspondientes deberán ser reservadas tal y como dispone el art. 112 LECRIM[27] para evitar que se ejerciten simultáneamente con el proceso penal, quedando su ejercicio reservado para ejercitarse posteriormente en la vía civil una vez finalizada la causa criminal.

Respecto a los medios de prueba que se recomienda a D. Daniel utilizar en este caso en el proceso penal para que se pueda demostrar que ha habido una cesión inconsentida de datos personales se utilizarán dos medios claros.

- Interrogatorio:
  El interrogatorio de la persona jurídica se realizará tal y como establece el art. 409bis LECRIM tomándose declaración al representante especialmente designado por la persona jurídica asistido de abogado, intentándose averiguar la participación de Facebook Spain en el presunto delito cometido tal y como se ha explicado anteriormente.
- Prueba electrónica (documental):

  Se habrán de introducir en el presente proceso la denominada prueba electrónica consistente en un registro de llamadas (oficiándose previamente a

---

[27] **Artículo 112.**

Ejercitada sólo la acción penal, se entenderá utilizada también la civil, a no ser que el dañado o perjudicado la renunciase o la reservase expresamente para ejercitarla después de terminado el juicio criminal, si a ello hubiere lugar.

Si se ejercitase sólo la civil que nace de un delito de los que no pueden perseguirse sino en virtud de querella particular, se considerará extinguida desde luego la acción penal.

la compañía telefónica para que indique los números de origen, fechas y duración de las llamadas recibidas), así como copia de los emails que D. Daniel ha recibido donde ha de figurar el nombre de la empresa que ha contactado con D. Daniel.

Como la LECRIM no hace referencia expresa a la valoración de la prueba electrónica en el proceso penal se habrá de estar ante lo dispuesto en el art. 741[28] de dicho texto legal en virtud del principio de libre valoración de la prueba, por lo que será de aplicación de manera supletoria lo dispuesto en el art. 382[29] LEC y 230.2[30] LOPJ.

Igualmente, será interesante acompañar la demanda de las pruebas documentales con las llamadas que D. Daniel ha recibido mediante un

[28] **Artículo 741:**

El Tribunal, apreciando según su conciencia las pruebas practicadas en el juicio, las razones expuestas por la acusación y la defensa y lo manifestado por los mismos procesados, dictará sentencia dentro del término fijado en esta Ley.

Siempre que el Tribunal haga uso del libre arbitrio que para la calificación del delito o para la imposición de la pena le otorga el Código Penal, deberá consignar si ha tomado en consideración los elementos de juicio que el precepto aplicable de aquél obligue a tener en cuenta.

[29] **Artículo 382. Instrumentos de filmación, grabación y semejantes. Valor probatorio.**

1. Las partes podrán proponer como medio de prueba la reproducción ante el tribunal de palabras, imágenes y sonidos captados mediante instrumentos de filmación, grabación y otros semejantes. Al proponer esta prueba, la parte deberá acompañar, en su caso, transcripción escrita de las palabras contenidas en el soporte de que se trate y que resulten relevantes para el caso.

2. La parte que proponga este medio de prueba podrá aportar los dictámenes y medios de prueba instrumentales que considere convenientes. También las otras partes podrán aportar dictámenes y medios de prueba cuando cuestionen la autenticidad y exactitud de lo reproducido.

3. El tribunal valorará las reproducciones a que se refiere el apartado 1 de este artículo según las reglas de la sana crítica.

[30] **Artículo 230.2:**

2. Los documentos emitidos por los medios anteriores, cualquiera que sea su soporte, gozarán de la validez y eficacia de un documento original siempre que quede garantizada su autenticidad e integridad y el cumplimiento de los requisitos exigidos por las leyes procesales.

documento acreditativo de dichas llamadas recibidas y del origen de las mismas (empresas o particulares que pudieran haber accedido a dichos datos personales de D. Daniel) el cual será solicitado a la compañía telefónica para que acredite el origen de dichas llamadas, las fechas, duración, etc. También se entregarán como pruebas documentales los emails publicitarios recibidos por D. Daniel donde figura el nombre de la empresa que ha contactado con él.

- Si D. Daniel decide seguir la vía judicial civil, debe iniciarla mediante la presentación de una demanda contra Facebook Spain, sita en Paseo de la Castellana, 35, 28046, Madrid. Los juzgados competentes serán los de Madrid, al ser Facebook Spain la responsable directa del tratamiento de los datos de los nacionales y usuarios españoles, y responsables de las acciones derivadas del mal uso de las mismas. En esta materia es de aplicación la Ley Orgánica 1/1982 de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

  Igualmente, y de acuerdo con el art. 18 de la Constitución Española, *se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen,* siendo protegido civilmente este derecho por la Ley Orgánica 1/1982 tal y como dispone su art. 1.

  Es importante en este punto tener en cuenta que la Ley Orgánica de protección del honor, intimidad y propia imagen es de 1982, por lo que internet apenas estaba desarrollado, pero se puede extrapolar todos los artículos y referencias a las escuchas e intromisiones y aplicarlos a los nuevos medios técnicos y tecnológicos que permiten acceder a esos datos y eventualmente vulnerar la intimidad personal. Es por ello por lo que las intromisiones ilegítimas en el ámbito de protección que se describen en el art. 7.2, 7.3, 7.4 y 7.5 de la Ley Orgánica 1/1982 son intromisiones que se rigen por lo dispuesto en esa Ley y por tanto ser procedimiento que fundamente el inicio de un proceso civil.

  En este caso, se está vulnerando la intimidad personal de D. Daniel, por lo que le es de aplicación lo dispuesto en esta Ley Orgánica 1/1982. Tal y como refiere el art. 9 de la Ley Orgánica 1/1982, la tutela judicial comprende la adopción de las medidas necesarias para poner fin a la intromisión ilegítima que se haya producido, restableciendo al perjudicado en el pleno disfrute de sus derechos, cesando inmediatamente de la intromisión y reponiéndolo al estado originario, de igual modo

se habrán de prevenir intromisiones inminentes o posteriores e indemnizar los daños y perjuicios causados, por lo que se habrá de solicitar la medida cautelar junto con el escrito de interposición de la demanda, tal y como indica el art. 730.1 LEC. Para ello se habrá de probar que dicha intromisión ilegítima se ha producido, por lo que se recomienda que D. Daniel proceda a grabar las llamadas telefónicas, así como a tener constancia de los emails recibidos, preguntando en todo momento a sus interlocutores de dónde han obtenido sus datos personales, pero recordando siempre que la caducidad de las intromisiones ilegítimas es de cuatro años desde que el legitimado pudiera haber ejercitado su derecho a reclamarlas[31].

Igualmente, el procedimiento que se habrá de seguir lo determina el art. 249.1.2º de la Ley de Enjuiciamiento Civil (LEC), por lo que, al tratarse de una tutela del derecho al honor, a la intimidad y a la propia imagen se sustanciará por los trámites del juicio ordinario, de acuerdo igualmente con la Sentencia del Tribunal Constitucional 81/2001, de 26 de marzo de 2001. La cuantía que se ha de reclamar se hará en concepto de indemnización por daño patrimonial y moral que se estime que ha sufrido D. Daniel.

De acuerdo con el art. 6 LEC, las personas jurídicas pueden ser parte en el procedimiento, por lo que Facebook Spain S.L, tiene capacidad para ser parte en cuanto tiene personalidad jurídica. Si es además responsable de los datos y del tratamiento que de los mismos se haga, puede ser demandada, es decir se puede interponer la demanda contra Facebook Spain S.L., compareciendo por dicha mercantil la persona que legalmente la represente (art. 7 LEC).

Respecto al lugar donde ha de ser demandada Facebook Spain S.L., es el art. 51 LEC el que dispone como norma o fuero de atribución de competencia el del domicilio del demandado, por lo que deberá ser demandada en su lugar de domicilio, dado que la opción que aporta dicho artículo para demandarla en el lugar donde la relación jurídica a que se refiera el litigio haya nacido o deba surtir efectos, siempre que haya sede, no es posible determinarlo en el caso concreto, por lo que habrá que demandar a la mercantil en Madrid, pudiendo señalarse el domicilio de la empresa o del apoderado, gerente o administrador de la misma tal y como señala el art. 155 LEC, a efectos de notificaciones.

[31] Sentencia del Tribunal Supremo de 7 de noviembre de 2019, ECLI: ES:TS:2019:3505.

Respecto a todos los procedimientos y las posibles vías de solución de este caso es interesante crear un nuevo apartado referido a los medios de prueba que se van a utilizar en este caso para que se pueda demostrar que ha habido una cesión inconsentida de datos personales de D. Daniel. Para ello se referirán las tres pruebas que se desean practicar:

- Interrogatorio:

  El interrogatorio de la persona jurídica se realizará tal y como establece el art. 309 LEC que se reproduce a continuación

  1. Cuando la parte declarante sea una persona jurídica o ente sin personalidad, y su representante en juicio no hubiera intervenido en los hechos controvertidos en el proceso, habrá de alegar tal circunstancia en la audiencia previa al juicio, y deberá facilitar la identidad de la persona que intervino en nombre de la persona jurídica o entidad interrogada, para que sea citada al juicio.

  El representante podrá solicitar que la persona identificada sea citada en calidad de testigo si ya no formara parte de la persona jurídica o ente sin personalidad.

  2. Cuando alguna pregunta se refiera a hechos en que no hubiese intervenido el representante de la persona jurídica o ente sin personalidad, habrá, no obstante, de responder según sus conocimientos, dando razón de su origen y habrá de identificar a la persona que, en nombre de la parte, hubiere intervenido en aquellos hechos. El tribunal citará a dicha persona para ser interrogada fuera del juicio como diligencia final, conforme a lo dispuesto en la regla segunda del apartado 1 del artículo 435.

  3. En los casos previstos en los apartados anteriores, si por la representación de la persona jurídica o entidad sin personalidad se manifestase desconocer la persona interviniente en los hechos, el tribunal considerará tal manifestación como respuesta evasiva o resistencia a declarar, con los efectos previstos en los apartados 1 y 2 del artículo 307.

- Prueba electrónica (documental):

  Igualmente, será interesante acompañar la demanda de las pruebas documentales con las llamadas que D. Daniel ha recibido mediante un documento acreditativo de dichas llamadas recibidas y del origen de las mismas (empresas o particulares que pudieran haber accedido a dichos datos personales de D. Daniel) el cual será solicitado a la compañía telefónica para que acredite el origen de dichas llamadas,

las fechas, duración, etc. También se entregarán como pruebas documentales los emails publicitarios recibidos por D. Daniel donde figura el nombre de la empresa que ha contactado con él.

CUARTO.-

Para responder la cuestión de contra quién debe D. Daniel dirigir sus peticiones, tal y como se ha analizado anteriormente, hay que diferenciar entre las tres vías procesales (contencioso-administrativo, penal y civil). Es por ello por lo que los pasos a seguir son los siguientes:

1. Reclamación extrajudicial previa y origen de la vía contencioso-administrativa:

   Se ha de interponer una reclamación extrajudicial previa por incumplimiento en la cesión de los datos personales ante la Agencia Española de Protección de Datos Personales.

   En primer lugar, se ha de contactar con el responsable de tratamiento de Facebook para poder ejercitar su derecho de acceso, rectificación, limitación, oposición, supresión, portabilidad y oposición al tratamiento de decisiones automatizadas. Tras ello podrá reclamar ante la AEPD por los medios y motivos expuestos anteriormente. Una vez que la AEPD valore el caso concreto de D. Daniel y dicte una resolución, contra ella cabrá recurso de reposición y extraordinario de revisión, una vez resueltos se podrá interponer recurso contencioso-administrativo[32] siguiendo los mecanismos que anteriormente se han detallado.

2. Vías civil y penal:

   Se ha de diferenciar entre el proceso penal y el proceso civil:

   2.1. Proceso penal:

   Desde el momento en que Facebook presenta una sede social en España bajo el nombre Facebook Spain S.L. y con domicilio en Paseo de la Castellana, 35B, 28046, Madrid cuyo objeto social es la gestión de las redes sociales, le es de aplicación lo dispuesto en el art. 15 LECRIM, lo que permite presentar la denuncia ante los Tribunales de Madrid, y esto basado en la especialidad del "domicilio del presunto reo" que la propia LECRIM prevé en su articulado. En este caso concreto la denuncia se interpondrá contra Facebook Spain, por el motivo de ser gestora de red social en internet según su objeto social como sede en territorio español, y por ello

[32] Sentencia del Tribunal Supremo, de 5 de febrero de 2019, ECLI: ES:TS:2019:487 y Sentencia del Tribunal Supremo de 10 de diciembre de 2019, ECLI: ES:TS:2019:1690.

responsables de los delitos que pudiera haber cometido por la cesión de datos personales inconsentida de Facebook. El domicilio del presunto reo, como representante, es el fuero que determina la competencia territorial del tribunal que ha de conocer de la causa, aunque se promueva contra una persona jurídica en este caso, según lo establecido en el art. 14bis LECRIM, siéndole de aplicación lo establecido en el art. 119 LECRIM, anteriormente reproducido.

La causa se tramita por el cauce del proceso penal abreviado según lo dispuesto en el art. 757[33] y siguientes LECRIM puesto que se trata de un delito que lleva aparejada una pena de privación de libertad es inferior a nueve años por ser un delito contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio recogidos en el Libro II, Título X del Código Penal, en concreto de una vulneración del art. 197.2 del texto legal anteriormente citado

2.2. Proceso civil:

Tal y como dispone el propio art. 6 LEC, las personas jurídicas pueden ser parte en el procedimiento, por lo que se interpondrá demanda contra Facebook Spain S.L., compareciendo por dicha mercantil la persona que legalmente la represente (art. 7 LEC).

Teniendo en cuenta que la actividad de tratamiento de los datos personales de los usuarios de la red social Facebook en el territorio geográfico correspondiente a España le corresponde a la mercantil Facebook Spain se habrá de presentar el escrito de demanda ante el Juzgado de Primera Instancia que por turno corresponda de Madrid, al tener la sede social dicha empresa en la Comunidad de Madrid (Paseo de la Castellana, 35), lo cual se establece en el art. 51 LEC, siendo la norma o fuero de atribución de competencia el del domicilio del demandado, pudiendo señalarse el domicilio de la empresa o del apoderado, gerente o administrador de la misma tal y como señala el art. 155 LEC.

[33] **Artículo 757.**

Sin perjuicio de lo establecido para los procesos especiales, el procedimiento regulado en este Título se aplicará al enjuiciamiento de los delitos castigados con pena privativa de libertad no superior a nueve años, o bien con cualesquiera otras penas de distinta naturaleza bien sean únicas, conjuntas o alternativas, cualquiera que sea su cuantía o duración.

QUINTO.-

Ante la pregunta de qué puede reclamar D. Daniel y la base jurídica o la fundamentación sobre la cual se pueden apoyar sus pretensiones es importante conocer que en el proceso civil se solicitará una restitución de sus derechos al honor y la intimidad personal, así como que le sea entregada como compensación por los daños y perjuicios causados por la cesión de sus datos personales por parte de Facebook a otras empresas.

Igualmente, en ambos procedimientos, se va a solicitar la detención de la cesión de sus datos de carácter personal, bien como medida cautelar, cosa que se recomienda que D. Daniel solicite en el escrito de interposición de la demanda del procedimiento civil, bien en el procedimiento penal.

En el caso del procedimiento penal, se imputa un posible delito del art. 197.2 del Código Penal a Facebook Spain, se ha de tener en cuenta que se recomienda a D. Daniel lo siguiente:

1. Declaración de los hechos constitutivos de un delito del art. 197.2 del Código Penal, dado que al haber pruebas de que D. Daniel únicamente ha indicado sus datos personales a la red social Facebook para poder crear una página con el fin de compartir su experiencia en viajes y otros hobbies, se estima que únicamente ha podido ser la red social Facebook la que haya podido ceder los datos de D. Daniel de modo inconsentido. Para ello se habrá de probar por los medios anteriormente expuestos que Facebook ha utilizado y comercializado los datos de carácter personal de D. Daniel sin su consentimiento para que terceros ajenos a Facebook puedan llevar a cabo las labores comerciales y de publicidad a las que se ha estado viendo sometido D. Daniel (se aportarán las pruebas correspondientes igualmente). De modo que Facebook, sin haber estado autorizado para tal fin de ceder los datos de D. Daniel a terceros, ha utilizado los datos reservados de carácter personal que estaban almacenados en un sistema informático (servidor de Facebook) en perjuicio de tercero, por lo que se constituye el delito de dicho artículo del Código Penal.
2. La reserva de acciones civiles para liquidarlas en el procedimiento correspondiente por la vía civil una vez finalizado el proceso penal, de este modo se logra que la compensación que D. Daniel pueda obtener por los daños y perjuicios causados sea mayor, dado que si esta misma se fija en el procedimiento penal la cuantía será menor.
3. Se solicitará que se respeten los derechos que D. Daniel tiene al acceso, rectificación, limitación, oposición, supresión, portabilidad y oposición al tratamiento de

decisiones automatizadas de sus propios datos personales, los cuales se ventilarán en el procedimiento judicial.

4. De igual modo, habrá de solicitar una serie de medidas cautelares acogiéndose a lo dispuesto en el art. 544 quáter LECRIM, entre ellas se le recomendará que sus datos personales sean borrados de cualquier base de datos a expensas de lo que pueda suceder durante el procedimiento penal.

Por ello, en el proceso penal se dirimirá la cuestión de si se ha cometido o no el delito del art. 197.2 del Código Penal.

En el caso del proceso civil por vulneración del derecho al honor y a la intimidad personal, al tramitarse por el procedimiento ordinario por razón de la materia, y atendiendo a lo establecido en la Ley Orgánica 1/1982, se han de formular varias pretensiones en el mismo escrito de demanda.

1. En primer lugar, se ha de solicitar la restitución de su derecho al honor y a la propia imagen mediante la detención de la cesión de datos no consentida tal y como dispone la propia Ley Orgánica 1/1982, una indemnización por los daños y perjuicios causados por dichas llamadas y correos electrónicos recibidos, así como por la cesión indebida y no consentida de los datos personales de D. Daniel.
2. En segundo lugar, se solicitará la condena en costas de la parte demandada.
3. En último lugar, se ha de solicitar una pretensión de condena en el propio escrito de interposición de la demanda, tal y como disponen los arts. 721 y siguientes LEC, solicitándose que sus datos personales sean cesados en el uso de manera temporal de cualquier base de datos en tanto el procedimiento no se dé por finalizado, para ello se ha de acoger a lo dispuesto en el art. 727.7 LEC, así como que de ponga fin a la intromisión ilegítima que se ha producido, restableciendo al perjudicado en el pleno disfrute de sus derechos, cesando inmediatamente de la intromisión y reponiéndolo al estado originario. De igual modo se habrán de prevenir intromisiones inminentes o posteriores e indemnizar los daños y perjuicios causados en caso de que dichas intromisiones no sean detenidas.

CONCLUSIONES

Como conclusión final a este trabajo se procede de exponer sintetizadamente las distintas respuestas a las cuestiones planteadas por D. Daniel.

1. ¿Ante qué organismo u organismos puede acudir para defender sus intereses?

   La defensa de sus propios intereses se puede llevar a cabo de varias maneras diferentes abordando cada una de ellas por distintas vías:

   - Reclamación directa ante el responsable del tratamiento de redes sociales de Facebook en Irlanda mediante escrito motivado y aportación de las pruebas de la existencia de dicha cesión de datos no consentida.
   - Reclamación ante la Comisión de Protección de Datos de Irlanda (no recomendada por su laxa legislación en esta materia), ante la OCU por vulneración de la normativa relativa a la Protección de Datos de Carácter Personal o ante la Agencia Española de Protección de Datos (recomendada) junto con la acreditación de que se ha reclamado ante Facebook el ejercicio de los derechos al acceso, rectificación, limitación, oposición, supresión, portabilidad y oposición al tratamiento de decisiones automatizadas ante el responsable del tratamiento de datos de Facebook. En caso de no estar de acuerdo con la resolución de la AEPD se puede iniciar la vía judicial contencioso administrativa mediante la presentación de recurso contencioso administrativo (una vez agotada la vía administrativa mediante la presentación, en su caso, de los recursos de reposición, y de revisión).
   - Denunciar a Facebook Spain por comisión del delito contra el derecho a la intimidad, del art. 197.2 del Código Penal que abre la vía penal y da origen al procedimiento abreviado por el que se protegerán los derechos de D. Daniel.
   - Demandar a Facebook Spain como responsable~~s~~ de la comisión de una intromisión ilegítima de la Ley Orgánica 1/1982 de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, vulneradora de su derecho fundamental a la intimidad, por la que se le reclama el cese del uso y disposición inconsentidos de sus datos personales, y una indemnización por daños y perjuicios que se le han ocasionado.

2. ¿Puede iniciar un pleito en defensa de sus intereses?

   D. Daniel puede iniciar un pleito en defensa de sus intereses por las tres vías antes contempladas:

   - La vía contencioso-administrativa contra la resolución de la AEPD.
   - La vía penal por la comisión del delito del art. 197.2 del Código Penal.
   - La vía civil en defensa de sus derechos al honor, la intimidad personal y familiar y a la propia imagen de la Ley Orgánica 1/1982, por la intromisión ilegítima concretada en el uso y disposición inconsentidos de sus datos personales.

3. ¿Ante qué tribunal o juez y dónde puede presentar un pleito en defensa de sus intereses al tratarse de una empresa multinacional?

   Dependiendo de la vía judicial elegida de las antes señaladas la competencia variará en función de la vía seleccionada:

   - Contra la resolución de la AEPD agotando la vía administrativa cabe recurso contencioso administrativo, que se ha de interponer ante la Sala de lo Contencioso Administrativo de la Audiencia Nacional tal y como establece la disposición adicional cuarta en su apartado quinto, así como los arts. 25, 46 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa.
   - Para iniciar el proceso penal se ha de presentar denuncia y desde el punto de vista territorial hay que estar a lo dispuesto en el art. 15 LECRIM que prevé que cuando no conste el lugar donde se haya cometido el delito serán competentes los Jueces y Tribunales de la residencia del presunto reo, en este caso Facebook Spain por sus labores y objeto social, por lo que se habrá de tramitar dicho proceso ante los tribunales de Madrid (Juzgado de Instrucción que por Turno Corresponda de Madrid).
   - La demanda del procedimiento civil se presentará ante los tribunales de Madrid (Juzgado de Primera Instancia que por Turno Corresponda de Madrid) según lo dispuesto en los arts. 51 y 155 LEC.

4. ¿Qué tipo de proceso será el pleito en defensa de sus intereses?

   El proceso para el pleito en defensa de sus intereses variará en función de la vía que se adopte:

   - En la vía contencioso-administrativa será el proceso contencioso administrativo.
   - En la vía penal será el proceso penal abreviado según lo dispuesto en el art. 757 LECRIM por imputarse la comisión de un delito que lleva aparejada una pena de privación de libertad inferior a nueve años.
   - En la vía civil será el denominado juicio ordinario, determinado por razón de la materia al tratarse de una vulneración del derecho al honor y a la intimidad personal de la Ley Orgánica 1/1982.

5. ¿Contra quién debe dirigir sus peticiones?

   Las peticiones de D. Daniel serán dirigidas a Facebook Spain S.L. en la vía penal y civil por ser responsable directo del almacenamiento y tratamiento de los datos personales de los usuarios de Facebook en España y por tanto responsable directo de dicha cesión inconsentida de los datos personales de D. Daniel.
   Sin embargo, si se inicia la vía de la reclamación extrajudicial ante la AEPD todas las peticiones deberán ser dirigidas a la propia Agencia de Protección de Datos por ser la tramitadora del expediente y actuando contra Facebook en nombre de D. Daniel.

6. ¿Qué puede reclamar?

   En todos los casos se va a atacar la cesión no consentida de los datos de carácter personal de D. Daniel, vulneradora de su derecho fundamental a la intimidad en su vertiente de derecho a los datos personales. En función del tipo de proceso que se vaya a llevar a cabo se reclamará lo siguiente:

   - En el proceso penal se reclamará una condena a Facebook Spain por la comisión del delito tipificado en el art. 197.2 del Código Penal, basando las pretensiones de D. Daniel en las pruebas que demuestran que se ha incurrido en el tipo de dicho delito puesto que D. Daniel únicamente ha prestado sus

datos personales para poder abrir la página de Facebook, siendo por tanto la mercantil la que ha cedido inconsentidamente los datos de D. Daniel y solicitando las pruebas que demuestren que se cumple el tipo, puesto que se han utilizado datos reservados de carácter personal que se hallan registrados en un soporte informático en perjuicio de terceros, cumpliendo por ello lo que el propio tipo penal establece.

- En el proceso civil se basarán las pretensiones de D. Daniel en la Ley Orgánica 1/1982, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Puesto que según el articulado de dicha ley se está vulnerando un derecho que el propio usuario tiene, y por ende da pie a que se puede solicitar una indemnización por los daños y perjuicios causados por dichas llamadas y correos electrónicos recibidos, así como por la cesión indebida y no consentida de los datos personales de D. Daniel, probando todo ello en el correspondiente proceso civil tal y como se ha expuesto anteriormente.
- En el proceso contencioso-administrativo se solicitará que se declare nula la resolución negativa (para los intereses de D. Daniel por la justificación que en la misma haya hecho la AEPD) y que se dicte una nueva resolución basada en las pretensiones de D. Daniel para la detención en la cesión inconsentida de sus datos personales.

CONCLUSIÓN PERSONAL

Como se ha podido observar a lo largo de toda la argumentación desplegada para la emisión de un dictamen fundado en relación con los hechos de este caso, de cesión no consentida de datos personales, la complejidad y magnitud de un hecho al que día a día cualquier usuario medio se expone en el uso de internet, es enorme. A mi juicio, es necesario que cualquier usuario de redes sociales comprenda que cuando se permite el acceso a los datos personales que esa persona aporta, dichos datos han de ser tratados de un modo concreto y cuidadoso, ya no solo en la propia red social, sino también en el uso de internet y de las cookies.

Un ejemplo real de la trascendencia de la información que trasmitimos al facilitar nuestros datos personales en las redes sociales sucedió durante las elecciones de 2016 de Estados Unidos y lo que se conoció como el escándalo de Cambridge Analytica[34]. Cambridge Analytica es una empresa británica que se creó en el año 2013 para realizar análisis y minería de datos con la intención de utilizar dichos datos con fines políticos como sucedió en la campaña presidencial de Donald Trump o en la votación sobre el Brexit. El caso se hace relevante cuando los datos que utilizan para su minería de datos proceden de métodos de obtención poco legítimos como los que se utilizaron en este caso concreto.

En el año 2013 Cambridge Analytica creó un test de personalidad bajo el nombre de Thisisyourdigitallife que se publicó en Facebook, siendo uno más de los test de personalidad que existen en dicha red social y que mucha gente realiza a modo de entretenimiento. El verdadero problema surge cuando para la realización de este test Cambridge Analytica paga a 270.000 usuarios de Facebook para que lo realicen, aparece así la cuestión de ¿por qué pagar a unos usuarios por hacerlos cuando estos test son muy comunes y se vuelven virales rápidamente? Pues en dicho pago se encuentra el asunto principal que causó el desplome en bolsa de Facebook y la declaración de Mark Zuckerberg ante el Senado de los Estados Unidos.

Cuando esos 270.000 usuarios realizaron ese test de personalidad desconocían que el mero hecho de hacer clic sobre dicho test de personalidad ya no solo estaba dando el acceso a los datos personales de esos 270.000 usuarios, sino que estaba permitiendo que los datos personales de los amigos de dichos 270.000 usuarios también fueran accesibles para

[34] Vercelli, A. (2018). *La (des) protección de los datos personales: análisis del caso Facebook Inc.-Cambridge Analytica.*

Cambridge Analytica, con lo que con el pago a 270.000 usuarios Cambridge Analytica se hizo con los datos de 87 millones de usuarios de la red social, siendo 71 millones de usuarios de Estados Unidos, con la intención de utilizar dichos datos personales en la próxima campaña electoral presidencial.

El cambio en la política de datos de Facebook en 2017 y la restricción de la API (Application Programming Interfaces, en español, interfaz de programación de aplicaciones) en 2014 no impidió que dichos datos fueran utilizados y que Cambridge Analytica tuviera acceso a las publicaciones, fechas de nacimiento, intereses, likes, ubicaciones, residencias, estados civiles, relaciones sentimentales, religión o multimedia, sino que también podían acceder a los mensajes personales de esos usuarios.

Se desconoce de cuál fue el uso exacto de todos esos datos, pero más adelante se realizaron auditorías y juicios que crean más dudas de las que despejan. Pero una cosa es importante, estamos ante unos mecanismos digitales que permiten que toda nuestra personalidad en internet sea conocida al menor descuido y que nuestros datos puedan ser utilizados sin haberlo consentido previamente.

A raíz de este escándalo, Facebook se volvió mucho más restrictivo y el cambio en su política de privacidad y tratamiento de datos se volvió mucho más intensa, por lo que un cambio a mejor sí que ha existido, pero aún desconocemos totalmente cómo nuestros datos se utilizan y son almacenados, confiando nuestra suerte a un ente incorpóreo al que se le ofrecen sin pedir a cambio más que unos cuantos "me gusta".

Cada día estamos más acostumbrados a lo que se denomina comúnmente correo basura dentro de nuestras carpetas de correo, pero lo ideal sería detenerse un momento y preguntarse: ¿cómo ha llegado esto hasta mi bandeja de entrada? Quizás vivimos en una sociedad en la que los datos personales no se valoran salvo cuando lo que se utiliza es nuestra imagen, y sin embargo, hay que advertir que eso es un escalón superior, dado que ahí ya no se está ante un supuesto delito de revelación de secretos, sino ante un delito contra el derecho a la propia imagen, y eso, lamentablemente, impide que valoremos que como individuos, consumidores, o usuarios en internet somos algo más que nuestras fotos, vídeos y publicaciones, somos una serie de datos, que, "inocentemente", regalamos a unas entidades que juegan con ellos, los comercializan y hacen de nosotros una moneda de cambio[35]. Es por ello por lo que la concienciación y el sentimiento de propiedad de sus propios datos que tiene

[35] Tello-Díaz, L. (2013). *Intimidad y «extimidad» en las redes sociales. Las demarcaciones éticas de Facebook*.

D. Daniel son esenciales para poder comprender hasta qué punto un individuo en internet no es sólo un dato más, y que sus datos, su nombre, su teléfono, sus actividades, ocios, hobbies, intereses, imágenes, vídeos y demás contenido es suyo y solo suyo, y como tal forma parte de su patrimonio en este caso personal o moral, cuya integridad y respeto ha de ser protegido por el ordenamiento jurídico.

BIBLIOGRAFÍA Y DOCUMENTACIÓN UTILIZADA

Agencia Española de Protección de Datos. *Informe 0197/2013*.

Agencia Española de Protección de Datos. *Informe 210070/2018*.

Agencia Española de Protección de Datos. *Informe sobre el interés legítimo en la protección de datos de carácter personal.*

Álvarez Hernando, J (2019). *Protección de datos personales en el proceso*. XII Congreso Nacional de la Abogacía.

Comité Europeo de Protección de Datos. *Guía 03/2019*.

Díaz, E. D. (2018). *Protección de datos: lecciones del caso Facebook. Nuestro tiempo*.

Dumortier, F. (2009). *Facebook y los riesgos de la «descontextualización» de la información*. IDP. Revista de internet, Derecho y Política, (9), 25-41.

Ramiro, M. A. (2005*). El derecho fundamental a la protección de datos personales en Europa* (Doctoral dissertation, Universidad de Alcalá).

Roa Navarrete, M. A. (2013). *Facebook frente al derecho a la vida privada y la protección de datos personales.*

Tello-Díaz, L. (2013). *Intimidad y «extimidad» en las redes sociales. Las demarcaciones éticas de Facebook*. Comunicar: Revista Científica de Comunicación y Educación, 21(41), 205-213.

Vercelli, A. (2018). *La (des) protección de los datos personales: análisis del caso Facebook Inc.-Cambridge Analytica*. In XVIII Simposio Argentino de Informática y Derecho (SID)-JAIIO 47 (CABA, 2018).

WEBGRAFÍA

Recursos contra una resolución de la Agencia Española de Protección de Datos (evamunoz.es)

¿Dónde guarda Facebook todos tus datos? (lavozdegalicia.es)

Información de la empresa | Información sobre Facebook (fb.com)

Conociendo los servidores de Facebook - Cuatro Círculos (cuatrocirculos.com)

https://ayudaleyprotecciondatos.es/2016/07/26/indemnizacion-aepd-lopd/

https://adsuarlegal.com/como-reclamar-una-indemnizacion-por-la-vulneracion-del-derecho-a-la-proteccion-de-datos/

https://elderecho.com/proteccion-datos-personales-proceso-penal-ii

https://www.elecelegal.com/proteccion-de-datos-vs-tutela-judicial-efectiva/

https://www.expansion.com/juridico/actualidad-tendencias/2018/03/27/5aba104446163ff2308b4653.html

https://auditoria-lopd.es/sancion-a-fb-y-whatsapp/

https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/la-aepd-sanciona-whatsapp-y-facebook-por-ceder-y-tratar

https://www.elperiodico.com/es/sociedad/20181011/ocu-demanda-facebook-cesion-irregular-datos-usuarios-7083655

https://www.elespanol.com/invertia/observatorios/digital/20181231/facebook-pagara-caros-errores-proteccion-datos/364214341_0.html

JURISPRUDENCIA

- Sentencia Lindqvist del Tribunal de Justicia de la Unión Europea (C101/01), de 6 de noviembre de 2003, ECLI:EU:C:2003:596
- Sentencia Nº 387/2009, Tribunal Supremo, Sala de lo Penal, Sección 1, Rec 1081/2008 de 13 de abril de 2009, ECLI: ES:TS:2009:3015.
- Sentencia Nº 221/2019, Tribunal Supremo, Sala de lo Penal, Sección 1, Rec 516/2018 de 29 de abril de 2019, ECLI: ES:TS:2019:1383.
- Sentencia Nº: 585/2012, Tribunal Supremo, Sala de lo Contencioso, Sección 6, Rec 23/2008 de 15 de julio de 2010, ECLI: ES:TS:2012:585
- Sentencia Nº 121/2019, Tribunal Supremo, Sala de lo Contencioso, Sección 3, Rec 627/2018 de 05 de febrero de 2019, ECLI: ES:TS:2019:487.
- Sentencia Nº 1690/2019, Tribunal Supremo, Sala de lo Contencioso, Sección 3, Rec 1644/2019 de 10 de diciembre de 2019, ECLI: ES:TS:2019:1690.
- Sentencia Nº 1562/2020, Tribunal Supremo, Sala de lo Contencioso, Sección 3, Rec 5479/2019 de 19 de noviembre de 2020, ECLI: ES:TS:2020:1562.
- Sentencia Nº 600/2019, Tribunal Supremo, Sala de lo Civil, Sección 1, Rec 5187/2017 de 07 de noviembre de 2019, ECLI: ES:TS:2019:3505.
- Auto Tribunal Supremo, Sala de lo Civil, Sección 1, Rec 1068/2017 de 13 de septiembre de 2017, ECLI:ES:TS:2017:7895A.
- Sentencia Nº 1579/2017, Tribunal Superior de Justicia de País Vasco, Sala de lo Social, Sección 1, Rec 1449/2017 de 11 de Julio de 2017, ECLI:ES:TSJPV:2017:2426.
- Sentencia Nº 2307/2017, Tribunal Superior de Justicia de Andalucía, Sala de lo Social, Sección 1, Rec 2776/2016 de 19 de Julio de 2017, ECLI:ES:TSJAND:2017:8169.
- Sentencia de la Audiencia Nacional , Sala de lo Contencioso, Sección 1, Rec 75/2017 de 11 de mayo de 2018, ECLI: ES: AN:2018:2264
- Sentencia Audiencia Nacional, Sala de lo Contencioso, Sección 1, Rec 548/2018 de 30 de octubre de 2020, ECLI: ES:AN:2020:3180.
- Sentencia Audiencia Nacional, Sala de lo Contencioso, Sección 1, Rec 948/2018 de 30 de octubre de 2020, ECLI: ES:AN:2020:3182.

- Sentencia Audiencia Nacional, Sala de lo Contencioso, Sección 1, Rec 786/2018 de 27 de diciembre de 2019, ECLI: ES:AN:2019:5188.
- Sentencia Audiencia Nacional, Sala de lo Contencioso, Sección 1, Rec 111/2018 de 06 de noviembre de 2019, ECLI: ES:AN:2019:5203.