



Se consulta si resulta conforme a lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, la utilización de un software que permite acceder a los perfiles de los usuarios de las redes sociales para descargar toda la información accesible para el usuario en cada red social. Según señala se trata de información abierta o alcanzable por la credencial (usuario de la red social) que emplea el robot. Se pretende con ello obtener y agregar la información que aparece publicada en una red social acerca de la actividad del usuario en todas las redes sociales en que participa, obteniendo así el perfil del usuario, ya que cada red puede dar un perfilado diferente y complementario. Se pretende obtener no solo la información del usuario sino del resto de usuarios que publican en ellas información accesible al usuario cuyo perfil se gestiona, así como las interacciones que existen entre los diversos usuarios.

Se consulta, si en caso de que no resulte legal si dicha herramienta puede ser utilizada por un detective privado o una agencia de detectives privados.

I

Para contestar a la consulta planteada debe tomarse en consideración, en primer lugar, la doctrina jurisprudencial del Tribunal Constitucional en esta materia que configura el derecho a la protección de datos como un derecho fundamental autónomo, diferenciado del derecho fundamental a la intimidad. Señala así en su Sentencia 292/2000 lo siguiente:

“De este modo, el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa



que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo.

La aludida Sentencia 292/2000 determina, asimismo, el contenido del derecho a la protección de datos personales señalando en su fundamento jurídico 7:

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

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



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

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, al regular dicho derecho establece en su artículo 1 que *“La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.”*

Por tratamiento de datos, debe entenderse conforme a lo establecido en el artículo 3.c) de la Ley Orgánica 15/1999 *“operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.”* De este modo, todas y cualquiera de las operaciones que se pretenden llevar a cabo con la herramienta a que se refiere la consulta, tanto la mera recogida de los datos, como su almacenamiento, consulta, comunicación, etc., constituyen tratamientos de datos personales que deberán someterse a lo establecido en la Ley Orgánica 15/1999.

Para que un tratamiento de datos sea conforme a lo previsto en la Ley Orgánica 15/1999 es preciso que dicho tratamiento sea acorde con las exigencias que la misma establece respetando los principios consagrados en dicha Ley y dando cumplimiento a las obligaciones que la misma impone a quien pretende tratar datos personales. .

Debe así analizarse si dicho tratamiento resulta respetuoso de los principios recogidos en el artículo 4 de la Ley Orgánica 15/1999, bajo el título calidad de datos. Debe aquí hacerse referencia en particular a los principios de proporcionalidad y finalidad recogidos en los números 1 y 2 de dicho artículo respectivamente. Dispone el artículo 4.1 que *“Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.”* El número 2 de dicho precepto establece que *“Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.”*



Cabe recordar que la proporcionalidad exige, según la doctrina del Tribunal Constitucional, siguiendo a tal efecto la sentada por el Tribunal Europeo de Derechos Humanos, la superación de un triple juicio, en el sentido de determinar si la medida adoptada es susceptible de conseguir el objetivo propuesto (juicio de idoneidad), si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad) y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto), es decir, si la injerencia producida en el titular del derecho objeto de restricción por la medida es la mínima en aras al logro del fin legítimo perseguido con aquélla.

Así pues la captación de datos personales solamente se encuentra justificada si persigue una finalidad determinada, explícita y legítima y, en tal caso, dicha captación de datos es idónea, necesaria y equilibrada o, en los términos, de la Ley Orgánica 15/1999, los datos recabados son adecuados, pertinentes y no excesivos para la consecución de tal finalidad. De este modo no cabe considerar que la finalidad de gestionar toda la información publicada por los individuos en una o varias redes sociales, constituya una finalidad explícita, determinada, legítima y proporcionada, por el contrario supone una fiscalización de las diversas actividades que las personas llevan a cabo en una o, en su caso, varias redes sociales, que comporta una restricción injustificada de su derecho a la privacidad, sin perjuicio de que pueda incidir en otros derechos fundamentales como los relativos al honor, a la intimidad personal y familiar y a la propia imagen o incluso en la libertad de movimientos o de expresión de las personas.

El hecho de que los datos hayan sido hecho públicos por los interesados no ampara su tratamiento en la forma pretendida en la consulta. Resulta aquí de interés la reciente sentencia 363/2017 de la Sala de lo Civil del Tribunal Supremo al señalar lo siguiente “ Que en la cuenta abierta en una red social en Internet, el titular del perfil haya "subido" una fotografía suya que sea accesible al público en general, no autoriza a un tercero a reproducirla en un medio de comunicación sin el consentimiento del titular, porque tal actuación no puede considerarse una consecuencia natural del carácter accesible de los datos e imágenes en un perfil público de una red social en Internet. La finalidad de una cuenta abierta en una red social en Internet es la comunicación de su titular con terceros y la posibilidad de que esos terceros puedan tener acceso al contenido de esa cuenta e interactuar con su titular, pero no que pueda publicarse la imagen del titular de la cuenta en un medio de comunicación.”

Dicha conclusión es igualmente aplicable al derecho fundamental a la protección de datos personales, de modo que el hecho de que una persona haya hecho públicos datos en una red social con la finalidad propia de uso de las redes sociales a que hace referencia dicha sentencia no supone una habilitación para que se utilicen los datos para hacer un seguimiento de la actuación de una persona en una o en todas las redes sociales de las que sea miembro, acumulando toda la información posible de la misma. Se quebrantaría así la prohibición de recoger datos por medios fraudulentos, desleales o ilícitos, establecida en el artículo 4.7 de la Ley, en tanto los usuarios de la red social tienen entre sus expectativas que los datos y contenidos que publican puedan ser vistos por otros usuarios de la red, con el grado de privacidad que en su configuración establezcan, pero no figura entre tales expectativas la de ser rastreados por un robot, sin su conocimiento ni consentimiento, que recoja y almacene masivamente las informaciones a ellos relativas, sus relaciones con otros usuarios de la red de que se trate y la interrelación de las informaciones a ellos referidas publicadas en otras redes sociales.

Se incumplen además otras obligaciones impuestas al responsable del fichero por la Ley Orgánica 15/1999, tales como la de dar cumplimiento al deber de información, exigido por el artículo 5 de la Ley Orgánica 15/1999, privando así al interesado de un elemento esencial del derecho a la protección de datos como es el de saber que sus datos se están tratando, por quién y con qué finalidad al objeto de que pueda ejercitar ante él los derechos que le reconoce la Ley Orgánica 15/1999.

Asimismo, no cabe un tratamiento de datos que no se encuentre legitimado en alguno de los supuestos contemplados en el artículo 6 de la Ley Orgánica 15/1999, de los cuales sólo resultaría de aplicación en el presente supuesto el relativo al consentimiento del interesado.

Cabe aquí mencionar que no cabe legitimar el tratamiento de datos pretendido en la consulta en lo dispuesto en el artículo 7.f) de la Directiva 95/46/CE, declarado de aplicación directa por la Sentencia del Tribunal de Justicia de la Unión Europea de 24 de noviembre de 2011, por la que se resuelven las cuestiones prejudiciales planteadas por el Tribunal Supremo en los recursos interpuestos contra el Reglamento de desarrollo de la Ley Orgánica 15/1999. Dispone dicho precepto que *“Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si (...) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y*



libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva” Ahora bien, en el presente supuesto tal y como anteriormente se ha señalado no cabe considerar que constituya un interés legítimo la acumulación de toda la información relativa a los individuos que figure en una o varias redes sociales.

Cabe, en este sentido hacer referencia a lo señalado por la Audiencia Nacional en su sentencia de 6 de junio de 2012, en que se pronuncia en los siguientes términos, respecto a la alegación formulada por una entidad de que concurría la causa legitimadora recogida en el artículo 7.f de la Directiva 95/46/CE:

“La invocada por la actora sentencia del Tribunal de Justicia de la Unión Europea de 24 de noviembre de 2011, dictada en una cuestión prejudicial planteada por el Tribunal Supremo respecto a la adecuación o no al derecho comunitario del artículo 10.2.b) del RDLOPD, contiene los siguientes pronunciamientos:

“1. Se opone al artículo 7.f) de la Directiva 95/46 la normativa nacional que, para permitir el tratamiento de datos, sin consentimiento, y necesario para la satisfacción de un interés legítimo (del responsable o del cesionario) exige que se respeten los derechos y libertades del interesado, y además que dichos datos figuren en fuentes accesibles al público, excluyendo de forma categórica y generalizada todo tratamiento que no figure en dichas fuentes.

2. El artículo 7, letra f) de la Directiva 95/46 tiene efecto directo”.

Pronunciamiento que se sustenta, entre otras, en las siguientes consideraciones:

“El artículo 7, letra f) establece dos requisitos acumulativos para legitimar el tratamiento de datos:

Necesario para satisfacer un interés legítimo.

Que no prevalezcan derechos y libertades fundamentales del interesado (Que requieran protección con arreglo al apartado 1 del Art. 1 de la presente Directiva).



El segundo requisito exige una ponderación de los derechos e intereses en conflicto que dependerá de las circunstancias concretas, teniendo en cuenta los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea.

A efectos de tal ponderación la lesión de los derechos fundamentales del afectado por el tratamiento puede variar en función de que los datos figuren ya, o no, en fuentes accesibles al público.

Los tratamientos que figuren en fuentes no accesibles al público implican necesariamente que el responsable o el cesionario del tratamiento dispondrán en lo sucesivo de cierta información sobre la vida privada del interesado. Lesión, más grave, de los derechos del interesado consagrados en los artículos 7 y 8 de la Carta que debe ser apreciada en su justo valor, contrarrestándola con el interés legítimo del responsable o del tercero”.

Es decir, conforme a la citada sentencia del Tribunal de la Unión Europea, en orden a evaluar la procedencia del tratamiento de datos personales sin consentimiento del afectado, a los efectos del citado artículo 7.f) de la Directiva 95/45 que tiene efecto directo, deben ponderarse dos elementos fundamentales:

El primero, si el tratamiento de los datos es necesario para satisfacer un interés legítimo (del responsable de los datos o del cesionario).

El segundo, si han de prevalecer o no los derechos fundamentales del interesado esencialmente referidos a la protección de sus datos personales.

Ponderación de intereses en conflicto, que como ya ha señalado esta Sección en la citada sentencia de 15 de marzo de 2012, dependerá de las circunstancias concretas de cada caso y en la que, no obstante, puede tomarse en consideración, como un elemento más de ponderación, el hecho de que los datos figuren ya en fuentes accesibles al público.



En el caso de autos, los datos de los denunciantes se encuentran registrados sin su consentimiento en un fichero denominado “Domicilios” que según la información actualizada a fecha 30 de junio de 2008 dispone de un número total de 36.812.617 registros, disponiendo todos ellos de fecha de nacimiento y de los que 3.442.902 disponen del dato del DNI -folios 180 a 184-. Dicho fichero aparece descrito en el Registro General de Protección de Datos como “Datos obtenidos de fuentes accesibles al público que sólo podrán ser consultados por empresarios acreditados con usuario y contraseña facilitados por la empresa previo pago de la cuenta”.

Se trata, por tanto de un fichero en el que se incluyen datos personales referentes a treinta y siete millones de afectados, en los que asociados a la mayoría de ellos figuran datos de gran importancia y trascendencia, como el DNI y la fecha de nacimiento, que no figuran en fuentes accesibles al público y, además, un domicilio actual y uno anterior y, en algunos casos, incluso información de las personas que conviven en el mismo domicilio que la que aparece registrada en el fichero, que tampoco figuran en fuentes accesibles al público.

La AEPD dictó en su día resolución que acuerda la inmovilización del citado fichero Domicilios, del que es responsable Saberlotodo y que obliga a la misma, a cesar en la utilización y cesión de los datos de carácter personal registrados en dicho fichero, así como a adoptar las medidas oportunas para que el acceso a la información que contiene quede imposibilita. Inmovilización que se acordó al amparo del artículo 49 LOPD, precepto que dispone “En los supuestos, constitutivos de infracción muy grave, de utilización o cesión ilícita de los datos de carácter personal en que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el Director de la Agencia Española de Protección de Datos podrá, además de ejercer la potestad sancionadora, requerir a los responsables de ficheros de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos. Si el requerimiento fuera



desatendido, la Agencia Española de Protección de Datos podrá, mediante resolución motivada, inmovilizar tales ficheros a los solos efectos de restaurar los derechos de las personas afectadas". Esta Resolución ha sido declarada ajustada a derecho por esta Sección en la SAN, de fecha 30 de abril de 2010 (Rec. 428/2009).

La Sala, a la vista de las circunstancias concurrentes expuestas, considera que debe prevalecer el derecho a la protección de datos de los denunciantes afectados incluidos en el citado fichero Domicilios, frente a los intereses particulares de la recurrente en explotar la citada base de datos que contiene nada menos que 37.000.000 de registros de datos personales, con la información asociada a los mismos ya indicada y recogida de la forma expuesta.

En efecto, no es lo mismo que una determinada empresa necesite averiguar el domicilio de una persona de la que es acreedora, a efectos de poder efectuar el cobro de la deuda (para lo cual y a efectos de satisfacer ese interés legítimo puede utilizar los medios adecuados y lícitos tendentes a averiguar ese nuevo domicilio y poder tratarlo en orden a dicha finalidad), que el hecho de la creación de un mega fichero como el que nos ocupa (que se reitera contiene 37.000.000 de registros de datos personales), con el fin de poder comercializarlo y ofrecer esa información obtenida. Además, como también se ha expuesto en algunos casos la información se asocia o abarca a las personas que conviven en el mismo domicilio que la que aparece registrada en el fichero, lo que conculca el derecho de protección de datos de los afectados.

Por tanto, debe concluirse que no concurre el interés legítimo alegado por la entidad recurrente (que obviamente no es la persona física o jurídica que puede tener interés en el cobro de las posibles deudas) para tratar y, en correlación, ceder dichos datos de carácter personal, debiendo prevalecer el derecho de los afectados a la protección de datos, por lo que deben entenderse cometidas las infracciones apreciadas por la resolución impugnada."



De todo lo anteriormente señalado cabe concluir que el tratamiento de datos pretendido en la consulta resulta contrario a lo previsto en la Ley Orgánica 15/1999, por incumplir los principios obligaciones y garantías en ella previstas.

II

Se consulta en segundo lugar si cabe utilizar dicha herramienta por un detective privado.

Debe aquí partirse de que la Ley 5/2014, de 4 de abril, de Seguridad privada, en su artículo 48 dispone que:

“1. Los servicios de investigación privada, a cargo de detectives privados, consistirán en la realización de las averiguaciones que resulten necesarias para la obtención y aportación, por cuenta de terceros legitimados, de información y pruebas sobre conductas o hechos privados relacionados con los siguientes aspectos:

a) Los relativos al ámbito económico, laboral, mercantil, financiero y, en general, a la vida personal, familiar o social, exceptuada la que se desarrolle en los domicilios o lugares reservados.

b) La obtención de información tendente a garantizar el normal desarrollo de las actividades que tengan lugar en ferias, hoteles, exposiciones, espectáculos, certámenes, convenciones, grandes superficies comerciales, locales públicos de gran concurrencia o ámbitos análogos.

c) La realización de averiguaciones y la obtención de información y pruebas relativas a delitos sólo perseguibles a instancia de parte por encargo de los sujetos legitimados en el proceso penal.

2. La aceptación del encargo de estos servicios por los despachos de detectives privados requerirá, en todo caso, la acreditación, por el solicitante de los mismos, del interés legítimo alegado, de lo que se dejará constancia en el expediente de contratación e investigación que se abra.

3. En ningún caso se podrá investigar la vida íntima de las personas que transcurra en sus domicilios u otros lugares reservados, ni podrán utilizarse en este tipo de servicios medios personales, materiales o técnicos de tal forma

que atenten contra el derecho al honor, a la intimidad personal o familiar o a la propia imagen o al secreto de las comunicaciones o a la protección de datos.

(...)

6. Los servicios de investigación privada se ejecutarán con respeto a los principios de razonabilidad, necesidad, idoneidad y proporcionalidad.”

Esta Agencia ha venido considerando lícito el tratamiento de datos de carácter personal que pueda derivarse de la realización de actividades de investigación privada, siempre que resulte ajustado a los principios de proporcionalidad y finalidad y siempre que quede circunscrita al ámbito del encargo en cuyo seno se desarrolla la actividad investigadora, que deberá igualmente respetar los citados principios. En este sentido se pronuncia, aunque de forma indirecta la sentencia de la Audiencia nacional de 20 de mayo de 2010, cuando afirma lo siguiente:

“Argumenta también (la recurrente) que viene actualizando los datos de los particulares contenidos en sus bases de datos mediante una mercantil dedicada a la seguridad privada y ningún detective privado tiene obligación de desvelar sus fuentes de información amparándose en el secreto profesional que asiste a su labor profesional. Argumentación que podría justificar, en su caso, la exención de la necesidad de consentimiento para la inclusión de los datos personales en los ficheros de tal empresa de detectives, pero no para la inclusión de los datos en los propios ficheros de la entidad sancionada, precisamente por tratamiento in consentido de datos en sus ficheros, que es (la recurrente) y no la empresa de detectives.”

En el mismo sentido, la sentencia de la Audiencia Nacional de 8 de marzo de 2012 afirma que *“esta Sala comparte la argumentación de la resolución impugnada en el sentido de considerar improcedente iniciar procedimiento sancionador, por infracción de la Ley de Protección de Datos, como consecuencia de la incorporación al procedimiento judicial de una prueba de video, realizada en la vía pública, por una agencia de detectives privados, en la que además de la imagen de la persona frente a quien se dirige el procedimiento, aparezcan también las de determinados familiares del mismo”*.

No obstante, como cabe apreciar en el texto reproducido en primer lugar y se desprende del segundo, la normativa de seguridad privada actualmente en

vigor no legitima cualquier tratamiento de datos por parte de los detectives privados, sino que dicho tratamiento queda limitado por dos principios especialmente relevantes: la existencia de un interés legítimo que justifique la realización de las tareas de investigación y la garantía de los derechos mencionados en el número 3 del artículo 48, entre los que figura el derecho a la protección de datos.

Cabe así señalar que para determinar si existe legitimación para un determinado tratamiento de datos por detectives privados deberá tenerse en cuenta si concurre una causa legitimadora en la persona o entidad que encarga el servicio de recogida de datos a los detectives privados, de modo que la recogida de datos será lícita en caso de que aquélla se encuentre legitimada para efectuar tal tratamiento de datos, no siéndolo en caso contrario. Debe así examinarse en cada caso concreto si existe legitimación para efectuar un determinado tratamiento, ahora bien, como se ha señalado en el presente informe carece de legitimación alguna una recogida masiva de datos como la pretendida con el software a que se refiere la consulta.