GEOLOCALIZACIÓN A TRAVÉS DE DIRECCIONES IP

GEOLOCALIZATION THROUGH IP ADDRESSES

Laura María Cabello Gil[1]

Resumen: La nueva tecnología y el avance de las comunicaciones ha variado la forma de delinquir, y asociado a ello, de investigar al delincuente. Son múltiples las variantes que la técnica pone a nuestra disposición para averiguar la ubicación de una persona, y no todas están recogidas por la norma o gozan de una regulación pormenorizada al respecto. Estamos ante un complejo y escaso entramado normativo que, en muy pocas ocasiones, hace referencia concreta a la geolocalización, y no es excepción a ello la obtención de datos a través de la dirección IP. Hemos de plantearnos cómo deben acceder las Fuerzas y Cuerpos de Seguridad del Estado a dicha información con total respeto a los derechos fundamentales de los ciudadanos, sin que se produzca vulneración alguna, con el objeto de poder usar la misma como fuente de prueba en el proceso penal.

Abstract: The new technology and the advancement of communications have changed the way of committing, and associated with, investigating the offenders. There are multiple variants that the technique puts at our disposal to find out the exact location of a person, and not all of them, are covered by the standard or have a detailed regulation in this regard. We are facing a complex and scarce normative framework that, in very few times, makes specific reference to the geolocation; the obtaining of data through the IP address isn't the exception of that rule. We should ask ourselves, how the Security Forces must access this information with full respect for the citizens

[1] Doctoranda de la Facultad de Derecho de la UNED. Directora de CA UNED Albacete y tutora de Derecho Penal: laucabello@albacete.uned.es

fundamental rights, avoiding any kind of violations, in order to get it as a source of proof in the penal process.

Palabras clave: Geolocalización, IP, rastreo policial, cesión de datos.

Keywords: Geolocalization, IP, police research, data transfer.

Recepción original: 12/12/2017
Aceptación original: 29/03/2017

Sumario: I. Introducción. II. Geolocalización a través de direcciones IP. III. Obtención y/o intervención de los datos IP por los investigadores. *III.A Rastreo policial de la IP. III.B Cesión de datos por los sujetos obligados*. IV. Conclusiones. V. Bibliografía. VI. Abreviaturas utilizadas.

I. INTRODUCCIÓN

La expansión de las redes de telecomunicaciones supone un importante desafío para la sociedad actual, en el sentido de encontrarnos ante procesos comunicativos en el entorno informático cada vez más complejos y sofisticados, que han superado con creces a la norma, y que necesitan de una protección jurídica actualizada ante las más que posibles amenazas emergentes en la conocida como sociedad de la información del siglo XXI. Contamos con sistemas GPS como dispositivos autónomos y como parte integrante de nuestro dispositivo de comunicación móvil, redes *WiFi*[2] que transmiten información de nuestra localización más allá de la que el ciudadano voluntariamente desea, archivos *Exif*en nuestras fotos que integran datos de la ubicación, estaciones base de telefonía que recogen de manera constante nuestra situación espacial... múltiples variantes que merecen ser analizadas ante la laguna jurídica existente y la escasa doctrina y jurisprudencia al respecto.

Vemos como nuestra sociedad actual es cada vez más dinámica y cambiante, y este hecho implica necesariamente la profundización en el análisis de los problemas jurídicos surgentes, con el objeto de adecuar el ordenamiento jurídico a las consiguientes transformaciones técnicas y sociales.

La evolución de la tecnología y el desarrollo de las comunicaciones supone la aparición de un nuevo campo de investigación para las

[2] *WiFi* o mecanismo de conexión de dispositivos electrónicos de forma inalámbrica.

Fuerzas y Cuerpos de Seguridad del Estado. Al igual que la delincuencia hace uso de los avances tecnológicos, las unidades de investigación se valen de ellos para perfeccionar su acción y acceder a información que tiempo atrás, era imposible.

No es necesario retroceder mucho en el tiempo para darnos cuenta del desarrollo inmenso que ha experimentado el campo de la geolocalización. Para conocer la ubicación de una persona, supuesto delincuente, las unidades de investigación únicamente contaban con los tradicionales seguimientos policiales, lo cual suponía un gran despliegue de medios personales y económicos. Actualmente, la tecnología pone en su mano multitud de herramientas para la averiguación de los ilícitos, y el ámbito de la geolocalización no se queda atrás.

Uno de los métodos de geolocalización usados por los investigadores son las direcciones IP. Primero se hace necesario partir de la concepción técnica de esta modalidad de localización, para posteriormente analizar la intervención y/u obtención de dichos datos para la investigación criminal con pleno respeto a los derechos fundamentales y a la legalidad vigente.

II. GEOLOCALIZACIÓN A TRAVÉS DE DIRECCIONES IP

La dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz (elemento de comunicación/conexión) de un dispositivo (un ordenador, un *Smartphone,* etc.) dentro de una red que utilice el protocolo IP (*Internet Protocol*[3]).

Para individualizar los millones de ordenadores existentes se utiliza esta dirección IP, la cual está compuesta por cuatro grupos de números, del 0 al 255, separados por puntos. Por tanto, la dirección IP no es más que un código de números de 32 bits que permite el establecimiento de una comunicación entre dos terminales informáticos o *hosts*.

Esta dirección IP es única y exclusiva para cada conexión, en el sentido de que no se puede acceder desde ningún ordenador a Inter-

[3] Internet Protocol (en español «Protocolo de Internet») o IP es un protocolo de comunicación de datos digitales clasificado funcionalmente en la Capa de Red según el modelo internacional OSI. Su función principal es el uso bidireccional en origen o destino de comunicación, para transmitir datos mediante un protocolo no orientado a conexión que transfiere paquetes conmutados a través de distintas redes físicas previamente enlazadas según la norma OSI de enlace de datos.

net sin tener adjudicada una dirección IP y no puede existir, al mismo tiempo, dos conexiones a Internet con la misma dirección IP.

La dirección IP es un recurso escaso con un número total disponible de cuatro mil millones de direcciones en todo el mundo, por lo que existe un organismo llamado ICANN (*Internet Corporation for Asigned Names and Numbers*) que es el encargado como autoridad internacional de definir los procedimientos y requisitos para delegar el uso de direcciones IP[4].

Los IPs pueden ser fijos o dinámicos. Los operadores asignan direcciones IP libres a aquellos clientes que precisen conectividad en ese momento (direccionamiento dinámico), en oposición al estático en el cual el cliente, esté conectado o no, siempre tiene la misma dirección IP. Actualmente, los IPs fijos son raros debido a razones de seguridad, ya que los ataques son más fáciles cuando el número de identificación de un terminal es siempre el mismo[5].

En cualquier caso, los números asignados como IP no son escogidos al azar, dependen del tipo de conexión que se utilice y desde donde se conecte el usuario, asignándose rangos de direcciones IP por zonas geográficas de forma ordenada, por lo que el servidor con el que se establezca una conexión, puede identificar aproximadamente el área desde donde se le efectúa la petición o lo que es lo mismo, la geolocalización del usuario.

---

[4] «*A nivel mundial existen 5 organismos regionales que ejecutan las directrices del ICANN en su región. La función más relevante es la asignación de direcciones IP. Cada uno de estos organismos dispone de un servicio (whois?) de consulta pública y gratuita, que permite obtener los datos del adjudicatario de una dirección IP y la forma de contacto.*

El organismo europeo responsable de ejecutar las directrices del ICANN se llama RIPE (Résseaux IP Européens). Este organismo es el que delega el uso de direcciones IP a los ISPs (proveedores de conectividad IP etc.), que deben satisfacer el pago de una cuota anual que dependerá del volumen de direcciones que contratan. La clave de la delegación es el uso responsable de un recurso escaso, por tanto, los operadores tendrán que justificar la necesidad de las IP´s que solicitan».

MARTÍNEZ GINESTA, G., «Límites técnicos de la ayuda prestada por las operadoras en la investigación de los delitos», en VELASCO NÚÑEZ, E., *Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia,* Consejo General del Poder Judicial, Madrid, 2007, pág. 114.

[5] La rotación de direcciones IPs (IP dinámicos) funciona de la siguiente forma: un determinado proveedor de acceso a Internet (Ej. Arnet), posee *x* números IPs para usar. Cada vez que una máquina se conecta a Internet, el proveedor le asigna una dirección IP aleatoria, dentro de una cantidad de direcciones IPs disponibles. El proceso más utilizado para esta distribución de IPs dinámicos es el *Dynamic Host Configuration Protocol* (DHCP). Para acceder a las URLs, o direcciones IPs públicos como conocemos (p.ej. www.boe.es), existen los servidores DNS (*Domain Name Server*), una base de datos responsable por la traducción de nombres alfanuméricos a direcciones IP, fundamentales para el funcionamiento de Internet, tal como la conocemos hoy.

III. OBTENCIÓN Y/O INTERVENCIÓN DE LOS DATOS IP POR LOS INVESTIGADORES

La Ley 9/2014, de 9 Mayo, General de Telecomunicaciones que si bien toca de manera muy tangencial e insuficiente a los datos de geolocalización, ofrece en su Anexo II –punto 9– una interesante definición de la geolocalización, presentando a los «Datos de localización», dentro de los cuales han de integrarse los obtenidos gracias a las direcciones IP, como cualquier dato tratado en una red de comunicaciones electrónicas o por un servicio de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público.

Descendiendo al tipo concreto de dato de geolocalización que nos ocupa, debemos de partir de la posición del Tribunal Supremo[6] en relación a la dirección IP. Su jurisprudencia afirma que la misma, si bien sí identifica a un ordenador determinado con una concreta conexión, no lo hace por sí respecto del usuario, por lo que estima que no se precisa autorización judicial para conseguir lo que es público, no encontrándose protegido ni por el apartado 1 ni por el 3 del artículo 18 de la Constitución Española[7].

Por tanto, la obtención de esa IP, en el sentido de conexión a Internet, no ha de considerarse como comunicación, y sí como presupuesto técnico necesario para hacerla posible[8].

Cuestión distinta de la conexión técnica como tal, son las subsiguientes actuaciones de identificación y localización de la persona que tiene asignado esa IP, ya que éstas sí se deben efectuar al amparo judicial, porque a diferencia de la dirección IP, el nombre del usuario al que corresponde es un dato proporcionado al proveedor en el mar-

[6] Sentencias del Tribunal Supremo, Sala Segunda, 292/2008, de 28 de mayo, y 776/2008, de 18 de noviembre.

[7] Recordemos que los apartados 1 y 3 del artículo 18 de la Constitución Española se refieren respectivamente al derecho al honor, a la intimidad personal y familiar y a la propia imagen, y al derecho al secreto de las comunicaciones.

[8] GONZÁLEZ LÓPEZ sostiene que «*entender que la conexión a Internet, que no necesariamente debe ir acompañada de una comunicación concurrente, constituye una comunicación es equiparable a sostener la condición de comunicación del envío de la señal a la antena de telefonía móvil a efectos de la ubicación del terminal en una área de cobertura. A nuestro entender, estas actuaciones técnicas, si bien pueden considerarse comunicación desde un punto de vista técnico, escapan al propósito ya apuntado de la comunicación (envío de mensaje emisor a receptor) y constituyen, por ello, un presupuesto técnico necesario para hacer posible la comunicación*».

GONZÁLEZ LÓPEZ, J. J., «Intervención de las comunicaciones: Nuevos desafíos, nuevos límites», en PÉREZ GIL, J. (Dir.) *El proceso penal en la sociedad de la información. Nuevas tecnologías para investigar el delito*, Editorial La Ley, Madrid, 2012, pág. 86.

co de una relación contractual sometido únicamente al régimen de protección de datos. Así, la averiguación de la dirección IP estática ha de considerarse como dato de suscripción, mientras que si fuera dinámica se hallaría vinculada a una comunicación concreta.

Lo anterior puede complicarse aún más, y ello sucede cuando se utiliza para la navegación por Internet una dirección IP de un servidor que no aporta datos sobre sus usuarios, de modo que se logra poner un intermediario entre el ordenador y la web o el servicio al que se accede, quedando únicamente en éste sólo los datos del servidor, pero no los del usuario. Estos intermediarios son conocidos como servidor *Proxy*[9].

En cualquier caso, y aunque no se hiciera uso de un *Proxy*, la dirección IP únicamente señalaría a un *router* a través del cual pueden acceder a Internet diversos ordenadores conectados al mismo tiempo, localizando el lugar desde el que se ha producido la conexión, pero en ningún caso el usuario, y quizás tampoco, si existen varios, el equipo concreto. Solo existe una posibilidad al respecto de la identificación del determinado terminal en uso, y es analizando la dirección MAC o identificador de la tarjeta red de la que cada ordenador dispone para conectarse a un *router*, pudiendo a veces dicha dirección viajar en algunos paquetes de información que se usan para la navegación por Internet, dato que podría ser muy útil en el seno de una investigación[10].

III.A Rastreo policial de la IP

En este punto es imprescindible desarrollar la postura del Tribunal Supremo en relación con la captación de la dirección IP, por parte

[9] «*Estos intermediarios son conocidos como servidor Proxy y sus direcciones IP pueden ser fácilmente encontradas en Internet tecleando «Proxy Server list» en cualquier buscador. Esta búsqueda nos redirigirá a multitud de páginas web, muchas de las cuales se encuentran establecidas en países como Rusia […]. Muchos de estos Proxy son ordenadores que por estar mal configurados permiten el acceso a usuarios anónimos […] pero otros muchos son servidores estratégicamente situados en países a los que resulta sumamente difícil acceder como Vietnam o China y en los que raramente se van a guardar los logs sobre las conexiones realizadas[…].*»

FERNÁNDEZ LÁZARO, F., «Medios técnicos en la investigación de los delitos informáticos», en VELASCO NÚÑEZ, E. (Dir.), *Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia*, Consejo General del Poder Judicial, Madrid 2007.

[10] La dirección MAC es un identificador hexadecimal de 48 bits que se expresa por seis pares de números hexadecimales, asignado directamente por el fabricante de los dispositivos y que no puede ser repetido, aunque sí modificado a través de una operación compleja conocida como *MAC Spoofing* haciendo uso de programas específicos o bien mediante el propio sistema operativo.

de unidades policiales especializadas en delitos tecnológicos, en los supuestos de accesos realizados por usuarios que se interconectaron con programas informáticos de intercambio de archivos con contenidos de pornografía infantil, a través de los cuales se obtenía información sobre las IP atribuidas a los usuarios[11].

Los usuarios así identificados intercambian gratuitamente sus archivos a través de programas P2P (*peer to peer*), los cuales permiten el acceso a sus terminales informáticos, así como la transmisión o copia de programas, archivos o documentos allí almacenados. Estos programas, tales como EMULE o EDONKEY, comparten nodos que interactúan entre sí facilitando el intercambio de toda clase de archivos de audio, video, *software*..., optimizando el rendimiento en la transferencia por su actuación global, donde no existen realmente ni servidores ni usuarios. Su éxito radica en que cualquier usuario de terminal informático puede adentrarse directamente en el contenido de todos los terminales interconectados con solo entrar en las direcciones web de los respectivos dominios P2P[12].

Es en esta dimensión abierta, del libre acceso consentido, donde la actuación policial ha tenido su encaje, plenamente lícito, a través de técnicas de rastreo de los accesos a los *hash* que contenían imágenes de pornografía infantil, y de los que se podía extraer, porque así lo publicaban junto con la imagen, los accesos que se habían producido a las mismas. Se trata de una información accesible a cualquier persona, un rastro dejado por los usuarios que accedían a tales contenidos, en condiciones tales que podía ser seguido por cualquier persona sin traba ni limitación alguna; pero a través de tal fuente solamente se puede acceder al dato impersonal, numérico, de determinada IP y de la hora y fe-

[11] Es en este ámbito delincuencial donde podemos encontrar la escasa jurisprudencia existente sobre este tema.

[12] Conforme a la sentencia del Tribunal Supremo, Sala Segunda, 167/2016, de 2 de marzo, «*la aplicación emule es una plataforma gratuita una plataforma gratuita ideada para el intercambio de archivos entre usuarios conectados a través de la misma, siendo uno de los denominados programas P2P (peer to peer), de los que existen diversas variantes en internet para las distintas redes de intercambio, todas ellas con funcionamiento semejante no existiendo un servidor central en el que se almacenan los contenidos y al que se pueda acceder para evitar su difusión, tratándose de una aplicación que no tiene clientes ni servidores fijos, y si uno de los usuarios inicia la descarga de un archivo, instantáneamente se convierte en servidor de la parte del archivo que ha descargado, posibilitando a un tercero iniciar la descarga simultanea desde su propia carpeta compartida del archivo incompleto recibido. Por tanto, y a grandes rasgos, la red emule es la unión de todos los usuarios de la misma, y los servidores, que son clientes con características especiales, permiten mantener a todos los clientes conectados unos con otros; y todo aquel que se instala un programa cliente de redes P2P forzosamente tiene que conocer que se trata de una red de usuarios que comparten parte de los contenidos de sus ordenadores.*»

cha del acceso, requiriéndose para el siguiente paso, para el conocimiento de la ubicación y de la persona que está detrás de tal acceso, de la previa autorización judicial para el recabo de tal información.

Así, en este entorno, se dicta la sentencia del Tribunal Supremo, Sala Segunda, 1058/2006, de 2 de noviembre, referida al empleo, no de redes P2P, sino de chats abiertos, accediendo a la información mediante el rastreo de las *file servers*. Un defecto de fondo en el contenido del recurso impidió al tribunal pronunciarse sobre la licitud del acceso a los números IP utilizados. Mismo problema hubo con la sentencia del Tribunal Supremo, Sala Segunda, 921/2007, de 6 de noviembre.

Continuando con esta temática del rastreo policial de la IP, la sentencia del Tribunal Supremo 236/2008, de 9 de mayo[13], se planteó «*la duda, de si para solicitar el número telefónico o identidad de una terminal telefónica (cabría extenderlo a una dirección o identificación de Internet: Internet protocols), es necesario acudir a la autorización judicial, si no han sido positivas las actuaciones policiales legítimas integradas por injerencias leves y proporcionadas, que puede respaldar la Ley Orgánica de Cuerpos y Fuerzas de Seguridad del Estado o Ley de Seguridad Ciudadana, en la misión de los agentes de descubrir delitos y perseguir a los delincuentes*», concluyendo que los datos identificativos de un titular o de una terminal deberían ser encuadrados, no dentro del derecho al secreto de las comunicaciones (artículo 18.3 de la Constitución Española), sino en el marco del derecho a la intimidad personal (artículo 18.1 de la Constitución Española) con las excepciones legales en relación a la necesidad de autorización judicial para recabar según qué datos[14].

Aun es más, quien utiliza un programa P2P asume que muchos de los datos se convierten en públicos para los usuarios de Internet, circunstancia que conocen o deben conocer los internautas, siendo asimismo dichos datos conocidos por la policía, datos públicos en internet, los cuales no se hallan protegidos por el artículo 18.1 ni por el 18.3 de la Constitución Española.

[13] Esta línea ha sido seguida por sentencias del Tribunal Supremo, Sala Segunda, tales como 292/2008, de 28 de mayo y 680/2010, de 14 de julio.

[14] LO 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal o su Reglamento, Real Decreto 1720/2007 de 21 de diciembre, que entró en vigor el 31 de marzo de 2008, sin despreciar la extinta Ley 32 de 3 de noviembre de 2003, General de Telecomunicaciones y su Reglamento, RD 424/2005 de 15 de abril de 2005, normativa que fue sustituida por la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, así como Ley 25/2007, de 18 de octubre de Conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicación, dictada en desarrollo de la Directiva de la Unión Europea 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo.

Así, la autorización, en opinión del Alto Tribunal, quedaría reservada para desvelar la identidad que hay detrás de la utilización de determinada dirección IP relacionada con un concreto acceso público.

Continúa con el mismo tenor, entre otras, la sentencia del Tribunal Supremo, Sala Segunda, 292/2008, de 28 de mayo[15], poniendo de manifiesto de manera destacable que «*la complejidad de la materia, su ductilidad, y las singulares características de la normativa que la regula, hace necesario que futuras resoluciones de esta Sala vayan perfilando un cuerpo de doctrina atendiendo a las peculiaridades de cada caso en concreto*».

Otras resoluciones del Alto Tribunal a este respecto, y que mantiene inalterada su postura de defender la licitud del rastreo policial de IP a través de lugares accesibles a cualquiera (redes P2P) en su labor de investigación criminal son las sentencias del Tribunal Supremo, Sala Segunda, 680/2010, de 14 de julio o la 247/2010, de 18 de marzo.

Mención concreta merece la sentencia del Tribunal Supremo 680/2010, de 14 de julio, ya que entra de lleno en la cuestión de la compatibilidad de la línea jurisprudencial anteriormente expuesta con las bases de datos relativos a las comunicaciones creados al amparo de la Ley 25/07 de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicación, y sienta la premisa de que tales bases de datos no excluyen la posibilidad de obtener la misma información por canales lícitos diversos, entre los que se encuentran, sin duda, aquellas fuen-

[15] Sentencia del Tribunal Supremo, Sala Segunda, 292/2008, de 28 de mayo, FJ9: «*cuando la comunicación a través de la Red se establece mediante un programa P2P, como en el EMULE o EDONKEY, al que puede acceder cualquier usuario de aquella, el operador asume que muchos de los datos que incorpora a la red pasen a ser de público conocimiento para cualquier usuario de Internet, como, por ejemplo el I. P., es decir, la huella de la entrada al programa, que queda registrada siempre. Y fue este dato, el I. P. del acusado, el que obtuvo la Guardia Civil en su rastreo de programas de contenido pedófilo, dato que –conviene repetir y subrayar– era público al haberlo introducido en la Red el propio usuario –el acusado– al utilizar el programa P2P. Por ello, no se precisa autorización judicial para conocer lo que es público, y esos datos legítimamente obtenidos por la Guardia Civil en cumplimiento de su obligación de persecución del delito y detención de los delincuentes, no se encuentran protegidos por el artículo 18.3 de la Constitución Española. Porque, debe recordarse, el I. P. del acusado que averiguó la Guardia Civil, no identifica la persona del usuario, lo que hace necesario para conocer el número del teléfono y titular del contrato la autorización judicial, que es lo que se hizo aquí, pues la Policía Judicial a través de un oficio de 6 de noviembre de 2005, completado por un informe de 24 de octubre del mismo año del Grupo de delitos telemáticos de la Guardia Civil interesa la preceptiva autorización que obtuvo con el libramiento de mandamiento judicial dirigido a los operadores de Internet para identificar ciertas direcciones IP del ordenador al objeto de proseguir la investigación.*»

tes que los propios usuarios hacen permeables, sin restricción alguna, al acceso a cualquier persona.

III.B Cesión de datos por los sujetos obligados

Consecuencia de la transposición de la Directiva 2006/24/CE[16], surge la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

Tras la entrada en vigor de esta Ley, se hace necesario el mandato judicial para oficiar a la operadora y que ésta proporcione la información relativa a una determinada IP[17], y ello pese a que el dato no pueda cobijarse bajo el manto protector del secreto de las comunicaciones.

Pese a las objeciones de la Fiscalía, que veía limitada con ello su capacidad de acción dentro de su función de promover la justicia, dado que sus peticiones de información a los operadores de servicios

[16] El artículo 1 de la Directiva 2006/24/CE fija como objeto de la misma armonizar las disposiciones de los Estados miembros relativas a las obligaciones de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones en relación con la conservación de determinados datos generados o tratados por los mismos, para garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro, siendo aplicable a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o al usuario registrado.

Esta Directiva 2006/24/CE ha sido anulada por la Sentencia del Tribunal de Justicia de la Unión Europea (STJUE), Gran Sala, de 8 de abril de 2014 debido a la escasa definición en la norma de las cautelas y garantías jurídicas precisas y claras que exige la inmisión en el derecho a la protección de datos personales.

Esta resolución del Tribunal de Justicia de la Unión Europea no determina la pérdida de validez de la norma española, ya que las Directivas, como herramientas de armonización o de acercamiento de las normas nacionales, no ostentan relación de interdependencia con éstas.

RODRÍGUEZ LAÍNZ, J. L., *Sobre la incidencia de la declaración de invalidez de la Directiva 2006/24/CE en la ley española sobre la conservación de datos relativos a las comunicaciones*, en La Ley Unión Europea, Diario La Ley, núm. 8308, Sección Doctrina, Ref. D-148, 12 de mayo de 2014.

[17] Antes de la aprobación de la Ley 25/2007, el artículo 12 de la Ley 34/2002, de 11 de Julio, de servicios de la sociedad de la información y de comercio electrónico (LSSICE) fijaba el marco jurídico para el tratamiento y la cesión de los datos, entre los que se hallaba la IP (derogado actualmente). Así, en su artículo 12 se establecía que estos datos quedaban a disposición de Jueces y Fiscales en el marco de investigaciones criminales o para la salvaguardia de la seguridad pública y la defensa nacional. Para el caso de las Fuerzas y Cuerpos de Seguridad del Estado, esta cesión se debía realizar de conformidad con la normativa de protección de datos de carácter personal.

serían denegadas, el Tribunal Supremo adoptó en línea continuista con la norma, el Acuerdo no Jurisdiccional, Sala Segunda, de 23 de febrero de 2010, en relación con esta necesidad de autorización judicial para la cesión de datos de las operadoras de comunicaciones, supliendo la laguna legal afirmando lo siguiente:

> «*Es necesaria la autorización judicial para que los operadores que prestan servicios de comunicaciones electrónicas o de redes públicas de comunicación cedan los datos generados o tratados con tal motivo. Por lo cual, el Ministerio Fiscal precisará de tal autorización para obtener de los operadores los datos conservados que se especifican en el art. 3 de la Ley 25/2007, de 18 de octubre*».

Sin perjuicio de que ha quedado clara la necesidad de actuación judicial, no lo es tanto la naturaleza de los datos que se recaban de los sujetos obligados. Así por ejemplo, para GONZÁLEZ LÓPEZ[18] si la obtención de la dirección IP se efectúa en el marco de una intervención de las comunicaciones, el conocimiento de los «datos de conexión» se vincula a comunicaciones determinadas, y debido a ello, se erigen como información comprendida en el secreto de las comunicaciones.

Por su parte, la sentencia del Tribunal Supremo, Sala Segunda, 247/2010, de 18 de marzo[19] que interpreta la doctrina existente, distingue entre los datos personales que pueden afectar al secreto a las comunicaciones, y cuándo los conservados y tratados por las operadoras, no se están refiriendo a comunicación alguna, es decir, datos estáticamente almacenados, conservados y tratados por operadores que se hallan obligados a la reserva frente a terceros. Así, presenta dos conceptos distintos:

a) datos personales externos o de tráfico que hacen referencia a una comunicación concreta y contribuyen a desvelar todo o parte del secreto que protege el artículo 18.3 de la Constitución Española.

b) datos o circunstancias personales referentes a la intimidad de una persona (artículo 18.1 de la Constitución Española), pero autónomos o desconectados de cualquier comunicación, que caerán dentro del derecho a la protección de datos informáticos o *habbeas data* del

[18] GONZÁLEZ LÓPEZ, J. J., «Intervención de las comunicaciones: Nuevos desafíos, nuevos límites», en PÉREZ GIL, J. (Dir.), *El proceso penal en la sociedad de la información. Nuevas tecnologías para investigar el delito*, *op.cit*., pág. 86.

[19] Que dice reconocerse heredera de las sentencias del Tribunal Supremo, Sala Segunda, 236/2008, de 8 de mayo, y 292/2008, de 28 de mayo, así como de la doctrina sentada en la sentencia del caso *Malone* (Sentencia del Tribunal Europeo de Derechos Humanos de 2 de agosto de 1984, caso Malone vs. Reino Unido).

artículo 18.4 de la Constitución Española[20] que no pueden comprometer un proceso de comunicación.

Aunque pudiera parecernos en una primera lectura que la sentencia está distinguiendo lo que podría definirse como la dimensión estática frente a la dinámica del dato relativo a las comunicaciones; lo cierto es que lo que hace realmente es romper con el principio de la protección formal del secreto de las comunicaciones, al establecer un auténtico criterio de exclusión de aquellos que se definen como datos personales externos o de tráfico, cuya menor incidencia en el secreto de las comunicaciones haría más adecuado residenciarlos en el ámbito de la protección de simples datos de carácter personal.

En este caso concreto (sentencia del Tribunal Supremo, Sala Segunda, 247/2010, de 18 de marzo), el Ministerio Fiscal, y no la policía, solicita la identidad del titular de un terminal informático, entendiendo la resolución que *los datos cuya obtención se pretende por el Fiscal no tienen relación ni afectan ni interceptan ni descubren ni tratan de descubrir una comunicación concreta, sino que por ser preciso para la acción investigadora el conocimiento del domicilio, número de teléfono o identidad del titular del terminal informático que opera en la Red (IP), la solicita a la operadora, al objeto de pedir del juez un mandamiento de entrada y registro con fines indagatorios o de investigación de un posible delito, acerca del que se conocen datos indiciarios*. Tal proceder del Ministerio Fiscal, declara el Alto Tribunal, no afecta al secreto de las comunicaciones, sino que se desenvuelve en el marco del derecho a la intimidad; más concretamente dada la escasa intensidad en que es efectuada, la cuestión se proyectaría sobre la obligación que establece la Ley Orgánica de Protección de Datos de no publicar los datos personales de los usuarios que un servidor de Internet posee, los cuales no pueden ceder-

[20] Recordado por PÉREZ GIL, el Tribunal Constitucional define este derecho en su sentencia 292/2000, FJ 5, como «*un derecho de control sobre los datos relativos a la propia persona. La llamada libertad informática es así el derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención*». La garantía opera sobre datos de muy diversa naturaleza, siempre que «*tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar o cualquier otro bien constitucionalmente amparado*» sentencia del Tribunal Constitucional 292/2000, FJ 6.

PÉREZ GIL, J., «El nuevo papel de la telefonía móvil en el proceso penal: ubicación y perfiles de desplazamiento», en PÉREZ GIL, J. (Dir.) *El proceso penal en la sociedad de la información. Nuevas tecnologías para investigar el delito,* Editorial La Ley, Madrid, 2012, pág. 150.

se sin el consentimiento del titular, aunque la ley establece diversas excepciones, entre las que se encuentra este supuesto[21].

Sin duda alguna, los datos relativos a la IP, como la localización, que pueden ser recabados de los sujetos obligados no son datos de tráfico ni tampoco gozan de la protección que otorga el artículo 18.3 de la Constitución Española, puesto que no están inmersos dentro de comunicación alguna, ni asociados a ella.

La ubicación de su regulación dentro de la Ley de Enjuiciamiento Criminal así lo avala, al encontrarse dentro de la Sección 3.ª del Capítulo V, Título VII del Libro II, y no de la Sección 2.ª dedicada a la *Incorporación al proceso de datos electrónicos de tráfico o asociados*. En refuerzo de nuestra posición, autores como VELASCO[22], el cual niega también que sea un dato de tráfico, la ubicación de la dirección IP como «datos contractuales asociados», entendiendo que continúan rigiéndose por la LOPD, ya que no son datos técnicos sino contractuales referentes a comunicaciones[23].

---

[21] El artículo 11.2 d) de la Ley Orgánica 15/1999 de 13 de diciembre nos dice que el consentimiento del interesado a que se refiere el párrafo anterior no será necesario.... d) «*Cuando la comunicación que deba efectuarse tenga por destinatario el Defensor del Pueblo, el Ministerio Fiscal, los Jueces o Tribunales o el Tribunal de Cuentas en el ejercicio de las funciones que tienen atribuidas*».

Por su parte la Ley 32/2003 de 3 de noviembre, General de Telecomunicaciones (aplicable en el supuesto que tratamos, y derogada por la Ley 9/2014, de 9 de mayo), cuyo articulado se remitía al art. 12 de la Ley 34/2002 de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (ahora derogada por la Ley 25/2007) establecía el deber de retención de datos de tráfico relativos a las comunicaciones electr*ónicas, más concretamente declaraba que* los «*datos se conservarán para su utilización en el marco de una investigación criminal o para la salvaguarda de la seguridad pública y la defensa nacional, poniéndola a disposición de los jueces o tribunales o del Ministerio Fiscal que así lo requieran*».

Actualmente, la vigente la Ley 9/2014, de 9 de mayo determina en su artículo 42 que *la conservación y cesión de los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación a los agentes facultados a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales se rige por lo establecido en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.*

[22] VELASCO NÚÑEZ, E., «Delitos cometidos a través de Internet. Cuestiones procesales», Primera Edición, Madrid, 2010, Editorial La Ley, pág. 149.

[23] Frente a ello, se erige MAEZTU que entiende que dicha línea de pensamiento dejaría sin contenido no solo a la Ley de Conservación de Datos, sino a la Directiva 2006/24/CE. Partiendo de la propia *ratio legis*, afirma que los datos que identifican a un usuario en relación a una IP, con independencia de que deban o puedan servir al ISP para prestar el servicio y para su facturación, es un tipo de datos sujeto a la LCD. El artículo 3 de la LCD expresamente dispone que: «*1. Los datos que deben conservarse por los operadores especificados en el artículo 2 de esta Ley, son los siguientes: […] a)*

Otro problema añadido que se ha planteado ha sido que conforme al objeto de la Ley 25/2007, de 18 de octubre, únicamente podrá autorizarse judicialmente la cesión de datos para aquellas investigaciones dedicadas a delitos graves[24]. Así, si nos fijamos, la gran mayoría de los delitos cometidos a través de Internet, se encuentran castigados con una pena de prisión menor a los cinco años[25], de modo que tanto los Juzgados de Instrucción como los investigadores se encuentran atados de pies y manos en estos supuestos. Resulta en cualquier caso paradójico que se admita la adopción de la prisión provisional, según el artículo 503.1 de la Ley de Enjuiciamiento Criminal, para delitos con penas iguales o superiores a dos años, o incluso menos en otros supuestos, y sin embargo, se requiera que el delito que se pretenda investigar a través de la cesión de datos sobre la IP esté castigado con pena mínima de cinco años de prisión.

En contestación a estas dudas, MAEZTU[26] recuerda varias argumentaciones jurídicas para superar o reinterpretar esa limitación legal, buscando una redefinición del concepto de delitos graves para poder así ampliar las posibilidades de investigación y de obtención de la identificación y localización del usuario de la dirección IP en aquellos supuestos de delitos con pena menor a los cinco años:

— la referencia a los delitos graves no es literal, puesto que esta clasificación de los delitos es extraño al resto de los ordenamientos jurídicos europeos. Visto así, la Directiva ha de ob-

---

Datos necesarios para rastrear e identificar el origen de una comunicación: […] 2.º Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet: […] iii) El nombre y dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo de Internet (IP), una identificación de usuario o un número de teléfono.»

MAEZTU LACALLE, D., «La identificación del titular de una dirección IP. Problemática en aplicación de la Ley 25/2007, de conservación de datos», en PÉREZ GIL, J. (Dir.) *El proceso penal en la sociedad de la información. Nuevas tecnologías para investigar el delito*, Editorial La Ley Madrid, 2012, pág. 213.

[24] Destacar que el legislador español, al utilizar el concepto de «... delitos graves contemplados en el Código Penal o en las leyes penales especiales», soluciona jurídicamente de manera correcta las necesidades de proporcionalidad exigidas por la sentencia del Tribunal de Justicia de la Unión Europea, Gran Sala, de 8 de abril de 2014.

[25] Conforme al Código Penal, por ejemplo los delitos de amenazas (artículo 169, únicamente las condicionales en su grado máximo alcanzarían los cinco años), difusión, venta o exhibición de material pornográfico entre menores de edad o incapaces (artículo 186), calumnias (artículo 206), injurias (artículo 209), o el delito de estafa (tipo básico, artículo 249).

[26] MAEZTU LACALLE, D., «La identificación del titular de una dirección IP. Problemática en aplicación de la Ley 25/2007, de conservación de datos», en PÉREZ GIL, J. (Dir.) *El proceso penal en la sociedad de la información. Nuevas tecnologías para investigar el delito*, *op.cit.*, pág. 215.

servarse bajo este condicionante que justifica la ampliación a delitos castigados con pena de menos de 5 años, puesto que de otro modo la transposición de la misma ha sido errónea.

— que el criterio usado por el del Código Penal para la clasificación de los delitos es meramente formal, y no material, y tiene como única finalidad ordenar procesalmente la atribución de competencias a las Audiencias Provinciales.

— que esta limitación a la investigación es una quiebra de la tutela judicial efectiva del artículo 24 de la Constitución Española, debiéndose tener en cuenta sentencias del Tribunal Constitucional, como la 104/2006, sobre la superación del concepto formal de los delitos graves.

Con la nueva regulación existente en la Ley de Enjuiciamiento Criminal, tras la reforma operada por Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, queda clara la consolidación de la línea jurisprudencial del Tribunal Supremo, y ello a la vista de su artículo 588 ter k, que prevé que cuando en el ejercicio de las funciones de prevención y descubrimiento de los delitos cometidos en internet, los agentes de la Policía Judicial tuvieran acceso a una dirección IP que estuviera siendo utilizada para la comisión algún delito y no constara la identificación y localización del equipo o del dispositivo de conectividad correspondiente ni los datos de identificación personal del usuario, solicitarán del juez de instrucción que requiera de los agentes sujetos al deber de colaboración, la cesión de los datos que permitan la identificación y localización del terminal o del dispositivo de conectividad y la identificación del sospechoso.

Ello no es óbice para que continúen las dudas, ya que al identificar la Ley Procesal los sujetos obligados al deber de colaboración en su artículo 588 ter e, se echa en falta que la norma prevea las frecuentes situaciones en las que el obligado a colaborar está fuera del territorio nacional y resulta, llamémosla asimismo dudosa por la falta de concreción, la previsión que realiza señalando como sujeto obligado a «*toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual*», lo cual adolece de la necesaria seguridad jurídica puesto que se manifiesta como un auténtico *cajón de sastre*.

IV. CONCLUSIONES

Los datos de geolocalización han sido tratados por la legislación, tanto nacional como europea, de manera sectorial sin darse cuenta de la pluridimensionalidad de su naturaleza, a veces de forma tangencial aprovechando regulaciones de otras materias, y siempre de manera insuficiente. Ello supone que se ha infravalorado su función como medida de investigación y su naturaleza como fuente de prueba, sin que parezca haberse percatado el legislador de la real trascendencia de estos datos, ya que incluso pueden suponer la afectación de un derecho fundamental en algunos casos.

La jurisprudencia y la doctrina tampoco han tratado los datos de geolocalización como un todo sino que, a tenor de determinados supuestos concretos, se han visto forzados a crear su posición al respecto, siempre superados por la realidad del avance de las tecnologías.

Dentro de esta pluridimensionalidad que caracteriza a los datos de geolocalización, nos encontramos con aquellos que son obtenidos a través de direcciones IP.

Los rastreos policiales para localizar direcciones IP pueden realizarse sin necesidad de autorización judicial, ya que no se trata de datos confidenciales preservados del conocimiento público cuando estamos ante un dato que el propio interesado ha permitido sea de público conocimiento[27], sin perjuicio de que se informe al Juez de Instrucción

---

[27] Sentencia del Tribunal Supremo, Sala Segunda, 292/2008, de 28 de mayo: «*No cabe negar que la Ley 25/2007, de 18 de octubre, de Conservación de Datos Relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones, da un paso de gigante –excesivo o desmesurado según la doctrina científica especializada–, al desarrollar la Directiva de la Unión Europea 2006-24 C. E. del Parlamento Europeo y del Consejo. Esta Ley tiene por objeto imponer la obligación a los operadores de telecomunicaciones de retener determinados datos generados o tratados por los mismos con el fin de entregarlos a los agentes facultados, en caso de que le fueran requeridos por éstos, entendiendo por tales agentes los pertenecientes a los Cuerpos Policiales, al Centro Nacional de Inteligencia y a la Dirección de Vigilancia Aduanera. Esta Ley exige para la cesión de estos datos, con carácter general, la autorización judicial previa y entre los datos que deben conservar figura el que es objeto del proceso que nos ocupa, es decir «la identificación del usuario asignada» en el acceso a Internet, como expresamente establece el art. 3.a.2.ºi), así como «el nombre y dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de protocolo de Internet (I. P.), una identificación de usuario o un número de teléfono». Por su parte, el art. 7 (procedimiento de cesión de datos) determina que los datos a los que se refiere el art. 3 necesitarán una resolución judicial para su cesión a los funcionarios policiales, con lo que, en principio, parece claro que la obtención del I. P. se encuentra sometida a esta exigencia, lo cual no resulta muy congruente con el hecho tantas veces repetido en esta resolución de que la obtención de ese dato por los servicios policiales se produjo lícitamente, con lo cual la incongruencia se convierte en absurdo cuando se requiere por*

competente si derivado de ello se solicita autorización judicial para intervención de las comunicaciones o registro de dispositivo.

Otra cosa distinta sería que no se vaya a realizar rastreo alguno, y se solicite a la autoridad judicial por parte de los investigadores, en el ejercicio de las funciones de prevención y descubrimiento de los delitos cometidos en internet, la identificación y localización del equipo o del dispositivo de conectividad correspondiente o los datos de identificación personal del usuario, para su requerimiento a los sujetos obligados por el deber de colaboración deber de colaboración debiéndose entonces cumplir lo dispuesto el artículo 588 ter k de la Ley de Enjuiciamiento Criminal.

En el momento presente, estando clara la necesidad de autorización judicial y que el delito investigado sea de los castigados con pena grave, como así expresamente se dispone en el articulado de la Ley, queda fuera todo tipo de interpretación extensiva, ya que la norma es clara al respecto. Dicho lo cual, ello no es óbice para que sea imprescindible reducir ese tope penológico que limita los delitos a investigar, dado que en la práctica se hace harto complicado la concesión de una autorización judicial para la investigación del titular de una IP siempre que se quiera ser riguroso con la norma; y una mayor concreción en los sujetos obligados por el deber de colaboración.

V. BIBLIOGRAFÍA

AGUAYO MEJÍA, J., «El derecho a la intimidad», en *Novedades jurisprudenciales en materia de derechos fundamentales,* Consejo General del Poder Judicial, Cuadernos Digitales de Formación, núm. 24, 2010.

ALCÁCER GUIRAO, R., *Derecho a la intimidad, investigación policial y acceso a un ordenador personal (Comentario a la STC 173/2011, de 7 de noviembre)*, en La Ley Penal, núm. 92, Sección Jurisprudencia del Tribunal Constitucional, Abril 2012.

BANACLOCLE PALAO, J., *Las diligencias de investigación restrictivas de los derechos fundamentales*, en «Aspectos fundamentales del derecho procesal penal», 1.ª Edición, Editorial La Ley, Madrid, 2010.

la norma una autorización judicial para acceder a un dato que el propio interesado ha permitido ser de público conocimiento. Cuestión distinta será en los supuestos en los que en las diligencias de investigación desarrolladas por las Fuerzas y Cuerpos Policiales en la persecución de actividades delictivas de cualquier naturaleza para cuyo progreso sea necesario conocer el IP (o el número telefónico) de una determinada persona que hasta el momento es desconocido, se tenga que acatar esa exigencia legal.»

ENERIZ OLAECHEA, F. J., *Derechos fundamentales y protección de los datos personales,* Consejo General del Poder Judicial, Cuadernos Digitales de Formación, núm. 29, 2012.

FERNÁNDEZ LÁZARO, F., «Medios técnicos en la investigación de los delitos informáticos», en VELASCO NÚÑEZ, E. (Dir.), *Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia*, Consejo General del Poder Judicial, Madrid, 2007.

GONZÁLEZ LÓPEZ, J. J., «Intervención de las comunicaciones: Nuevos desafíos, nuevos límites», en PÉREZ GIL, J. (Dir.) *El proceso penal en la sociedad de la información. Nuevas tecnologías para investigar el delito*, Editorial La Ley, Madrid, 2012.

MAEZTU LACALLE, D., «La identificación del titular de una dirección IP. Problemática en aplicación de la Ley 25/2007, de conservación de datos», en PÉREZ GIL, J. (Dir.) *El proceso penal en la sociedad de la información. Nuevas tecnologías para investigar el delito*, Editorial La Ley, Madrid, 2012.

MARTÍNEZ GINESTA, G., «Límites técnicos de la ayuda prestada por las operadoras en la investigación de los delitos», en VELASCO NÚÑEZ, E., *Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia*, Consejo General del Poder Judicial, Madrid, 2007.

PÉREZ GIL, J., «El nuevo papel de la telefonía móvil en el proceso penal: ubicación y perfiles de desplazamiento», en PÉREZ GIL, J. (Dir.) *El proceso penal en la sociedad de la información. Nuevas tecnologías para investigar el delito*, Editorial La Ley, Madrid, 2012.

RODRÍGUEZ LAÍNZ, J. L., «Dirección IP, IMSI e intervención judicial de comunicaciones electrónicas», en *Diario La Ley,* núm. 7086, Sección Doctrina, 2 enero 2009, Año XXIX.

— «Dirección IP, IMSI e intervención judicial de comunicaciones electrónicas», en *Estudios sobre el secreto de las comunicaciones. Perspectiva doctrinal y jurisprudencial*, edición núm. 1, Editorial La Ley, Madrid, 2011.

— *Sobre la incidencia de la declaración de invalidez de la Directiva 2006/24/CE en la ley española sobre la conservación de datos relativos a las comunicaciones*, en La Ley Unión Europea, Diario La Ley, núm. 8308, Sección Doctrina, Ref. D-148, 12 de mayo de 2014.

ROMEO CASABONA, C. M.ª, «De los delitos informáticos al Cibercrimen. Una aproximación conceptual y político-criminal», en *El Cibercri-*

men: Nuevos retos jurídico-penales, nuevas respuestas político criminales, Editorial COMARES, Granada, 2006.

RUBÍ NAVARRETE, J., *Tratamiento de datos en el sector de las telecomunicaciones*, en INAP (Ministerio de Hacienda y Función Pública), Cuadernos de Derecho Público, núm. 19-20, mayo-diciembre 2003.

SALOM CLOTET, J., «Delito informático y su investigación», en VELASCO NÚÑEZ, E. (Dir.), *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?*, Cuadernos de Derecho Judicial, núm. 3, Consejo General del Poder Judicial, Madrid 2006.

VELASCO NÚÑEZ, E., «Delitos cometidos a través de Internet. Cuestiones procesales», Primera Edición, Editorial La Ley, Madrid, 2010.

VI. ABREVIATURAS UTILIZADAS

Art.	Artículo.
C.E.	Comunidad Europea.
ICANN	Internet Corporation for Asigned Names and Numbers.
IP	Internet Protocol.
L	Ley.
LCD	Ley de Conservación de Datos.
LO	Ley Orgánica.
LOPD	Ley Orgánica de Protección de Datos.
P2P	Peer to peer.
RD	Real Decreto.
STEDH	Sentencia del Tribunal Europeo de Derechos Humanos.
STJUE	Sentencia del Tribunal de Justicia de la Unión Europea.