Gabilex

Nº 43
Tercer trimestre 2025

REVISTA DEL GABINETE JURÍDICO DE CASTILLA-LA MANCHA

REVISTA DEL GABINETE JURÍDICO

DE CASTILLA-LA MANCHA

Número 43. Septiembre 2025

Revista incluida en Latindex, Dialnet, MIAR, Tirant lo Blanch

Solicitada inclusión en SHERPA/ROMEO, DULCINEA y REDALYC

Disponible en SMARTECA, VLEX y LEFEBVRE-EL DERECHO

Editado por Vicepresidencia

D.L. TO 862-2014

ISSN 2386-8104

revistagabinetejuridico@jccm.es

DIRECCIÓN

CONSEJO DE REDACCIÓN

COMITÉ CIENTÍFICO

D. Salvador Jiménez Ibáñez

Ex Letrado Jefe del Gabinete Jurídico de la Junta de Comunidades de Castilla-La Mancha.

Ex Consejero del Consejo Consultivo de Castilla-La Mancha.

D. José Antonio Moreno Molina

Catedrático de Derecho Administrativo de la Universidad de Castilla-La Mancha.

D. Isaac Martín Delgado

Profesor Dr. Derecho Administrativo de la Universidad de Castilla-La Mancha.

Director del Centro de Estudios Europeos *"Luis Ortega Álvarez".*

CONSEJO EVALUADOR EXTERNO

D. José Ramón Chaves García

Magistrado de lo contencioso-administrativo en Tribunal Superior de Justicia de Asturias.

Dª Concepción Campos Acuña

Directivo Público Profesional.
Secretaria de Gobierno Local

D. Jordi Gimeno Beviá

Prof. Derecho Procesal de la UNED

D. Jorge Fondevila Antolín

Jefe Asesoría Jurídica. Consejería de Presidencia y Justicia. Gobierno de Cantabria.
Cuerpo de Letrados.

D. David Larios Risco

Letrado de la Junta de Comunidades de Castilla-La Mancha.

D. José Joaquín Jiménez Vacas

Funcionario de carrera del Cuerpo Técnico Superior de Administración General de la Comunidad de Madrid

D. Javier Mendoza Jiménez

Doctor en Economía y profesor ayudante doctor de la Universidad de La Laguna.

SUMARIO

EDITORIAL

En el número 43 de la Revista Gabilex, se incluyen en la sección nacional seis artículos doctrinales que se suman a un artículo de la sección internacional y una reseña de jurisprudencia todos ellos de máximo interés.

En primer lugar, debe destacarse el excelente trabajo de D. Luis S. Moll Fernández- Fígares con el artículo que lleva por título "Inteligencia Artificial, Llull y el Ars Magna. Historia de la computación". El autor incide en la idea de una IA no es de generación espontánea, en el siglo XX, sino que es el resultado de la evolución del pensamiento y de una aspiración humana de más de siete siglos de antigüedad

El siguiente artículo que podrán disfrutar los lectores corresponde a Dª Laura Sánchez de Rivera García con el artículo que lleva por título "La declaración extemporánea del investigado durante la instrucción".

A continuación, Dª Lena Carazo Sánchez realiza un estudio brillante sobre "La investigación penal digital: OSINT, direcciones IP y el equilibrio entre eficacia y derechos fundamentales".

Dª Gema María Ortega Expósito aborda bajo el título "La contratación pública electrónica a la luz de la normativa europea. Especial referencia a las plataformas electrónicas. Historia reciente, presente y propuestas

para el futuro" un análisis de la evolución histórica de la regulación europea de la contratación pública electrónica en la Unión Europea, haciendo alusión a la tercera y cuarta generación de directivas y proponiendo nuevas medidas a incluir en la futura normativa europea, con el objeto de reforzar y ampliar el carácter obligatorio de las formas digitales en la contratación.

A continuación, D. David Quiralte Miguel aborda un tema de máximo interés con el artículo doctrinal "La resolución bancaria" la regulación a nivel español y europeo, con énfasis en la Unión Bancaria Europea y el Mecanismo Único de Resolución (MUR).

La sección nacional se cierra con la obra de Dª Miriam Romero Saiz sobre "Dictamen jurídico sobre la tramitación del concurso sin masa y obtención de la exoneración del pasivo insatisfecho a próposito de la entrada en vigor de la ley 16/2022, de 5 de septiembre, de reforma del texto refundido de la ley concursal" Un interesante artículo en el que aborda el desarrollo de un procedimiento concursal de dos personas físicas a propósito de la entrada en vigor de la Ley 16/2022, de 5 de septiembre, de reforma del texto refundido de la Ley Concursal.

Dª Paloma Cascales Bernabeu realiza la reseña jurisprudencial titulada "¿Pueden las víctimas recurrir revisiones de condena? Una mirada constitucional a la STC 105/2025, de 29 de abril".

Se centra en el pronunciamiento reciente del Tribunal Constitucional que analiza el derecho de las víctimas a recurrir revisiones de sentencias firmes, en el contexto

de la aplicación de la Ley Orgánica 10/2022. La reseña examina los fundamentos constitucionales de la decisión, su conexión con el artículo 24 CE, y su relevancia desde una perspectiva de género y de justicia restaurativa.

La sección internacional cuenta con el excelente trabajo de D. Adriano da Silva Ribeiro y de D. Estevão Grill Pontone que hará las delicias de los lectores sobre "Cláusulas de resolución de controversias y su aplicación en el derecho social".

El Consejo de Redacción

REVISTA DEL GABINETE JURÍDICO DE CASTILLA-LA MANCHA

SECCIÓN NACIONAL

ARTÍCULOS DOCTRINALES

Gabilex

Nº 43

Septiembre 2025

https://gabinetejuridico.castillalamancha.es/ediciones

LA INVESTIGACIÓN PENAL DIGITAL: OSINT, DIRECCIONES IP Y EL EQUILIBRIO ENTRE EFICACIA Y DERECHOS FUNDAMENTALES

DIGITAL CRIMINAL INVESTIGATION: OSINT, IP ADDRESSES, AND THE BALANCE BETWEEN EFFECTIVENESS AND FUNDAMENTAL RIGHTS

Dª. Lena Carazo Sánchez
Egresada del Doble Grado en Derecho y en Ciencia Política y Administración Pública de la Universidad de Salamanca

Resumen: La transformación digital ha cambiado profundamente la forma de entender la investigación penal, dando lugar al uso generalizado de herramientas tecnológicas como la Inteligencia de Fuentes Abiertas (OSINT) y la obtención de direcciones IP como formas de diligencias de investigación. Estas técnicas, al no requerir autorización judicial en muchos casos, han incrementado la eficiencia investigadora, pero también han generado importantes dilemas jurídicos y éticos. Este trabajo analiza críticamente el uso de ambas herramientas en el contexto español y europeo, comparándolas con la interceptación tradicional de las

comunicaciones y evidenciando el choque que se produce con ciertos derechos fundamentales. A través del estudio de la legislación, la jurisprudencia y los recientes desarrollos normativos de la Unión Europea, se evidencian las lagunas legales actuales y se proponen reformas orientadas a garantizar un equilibrio entre eficacia policial y respeto a los derechos fundamentales, especialmente la intimidad y el secreto de las comunicaciones.

Palabras clave: investigación policial digital, OSINT, dirección IP, derechos fundamentales, privacidad, LECrim, interceptación de las comunicaciones telefónicas y telemáticas.

Abstract: The digital transformation has profoundly changed the way criminal investigations are understood, leading to the widespread use of technological tools such as Open Source Intelligence (OSINT) and IP address tracing as forms of investigative proceedings. These techniques, which in many cases do not require judicial authorization, have increased investigative efficiency but have also raised significant legal and ethical dilemmas. This paper critically analyzes the use of both tools within the Spanish and European context, comparing them to the traditional interception of communications highlighting the conflict that arises with certain fundamental rights. Through the study of legislation, jurisprudence and recent regulatory developments in the European Union, current legal gaps are identified, and reforms are proposed to ensure a balance between police effectiveness and respect for fundamental rights, particularly privacy and the confidentiality of communications.

Keywords: digital criminal investigation, OSINT, IP address, fundamental rights, privacy, LECrim, interception of telephone and telematic communications.

Sumario:

I. INTRODUCCIÓN

La investigación policial en la era digital supone un cambio en el paradigma hasta ahora establecido. Los métodos clásicos de investigación se han quedado obsoletos en un contexto donde gran parte de la actividad humana se desarrolla en entornos digitales. Esto ha transformado no solo las relaciones personales, sino también el modo en que se cometen, investigan y persiguen los delitos. Este nuevo escenario se ve reflejado en datos recientes: a comienzos de 2025, más de 5.640 millones de personas, lo que equivale al 68,7% de la población mundial, estaban conectadas a Internet[1]. La conectividad global genera a diario inmensas cantidades de datos que recogen cada interacción de los

[1] Según datos de *DataReportal,* "Digital around the Word". Disponible en: https://datareportal.com/global-digital-overview

usuarios en la red. Esto es lo que ha convertido a Internet en el principal espacio donde rastrear indicios sobre conductas delictivas y sobre los posibles autores de un delito. Es tal la importancia de la investigación policial digital, que se estima que se utilizan datos electrónicos en el 85% de las investigaciones penales en la Unión Europea[2]. Esta cifra no solo confirma el desplazamiento del foco de la investigación hacia el ámbito digital, sino que demuestra que la tecnología no es un recurso accesorio, sino uno principal en el desarrollo de las diligencias de investigación actuales.

Esta incorporación de las nuevas tecnologías a las diligencias de investigación ha traído consigo ventajas significativas en relación con la agilidad, eficiencia y disponibilidad de información. Sin embargo, la digitalización de las investigaciones también plantea nuevos desafíos derivados de este gran volumen de datos, la complejidad de las herramientas digitales y del respeto a los principios básicos del proceso. Estos retos derivan de la capacidad para acceder y procesar información en línea sin límites, y sin un control riguroso que garantice el respeto a los derechos fundamentales.

La reforma de la Ley de Enjuiciamiento Criminal llevada a cabo por la Ley Orgánica 13/2015 ha supuesto un gran avance a la hora de actualizar la legislación a la investigación digital, sin embargo, aspectos novedosos de este tipo de investigación quedan fuera de este encuadre normativo y hace que se generen importantes

[2] Datos recabados del análisis del Consejo de la UE y del Consejo Europeo: "Mejor acceso a las pruebas electrónicas para combatir la delincuencia", (2024). Disponible en: https://www.consilium.europa.eu/es/policies/e-evidence/

dilemas jurídicos y éticos en relación con los derechos fundamentales reconocidos en la Constitución Española, especialmente aquellos vinculados a la intimidad, el secreto de las comunicaciones y la protección de datos personales. En este trabajo nos vamos a centrar en dos técnicas clave de la investigación policial digital, la Inteligencia de Fuentes Abiertas (OSINT) y la identificación mediante direcciones IP. Ambas se han consolidado como herramientas cada vez más frecuentes en las diligencias policiales, por centrar su actuación en el entorno digital. En el caso de la OSINT, su relevancia se acentúa por el uso intensivo de las redes sociales, donde aproximadamente el 63,9% de la población mundial mantiene una actividad regular[3], lo que convierte estas plataformas en espacios clave para la obtención de información relevante en el curso de una investigación. Por lo que el objeto central de este trabajo es analizar críticamente estas dos técnicas, evaluando su encuadre en el marco jurídico español y europeo, así como su impacto en los derechos fundamentales y proponer una solución ante la actual situación regulatoria.

La relevancia de esta investigación se justifica por la creciente necesidad de encontrar un punto de equilibrio entre la eficacia en la lucha contra la delincuencia y la obligación de preservar los derechos fundamentales en un entorno digital donde la recopilación masiva de datos puede suponer una intromisión desproporcionada en la vida privada tanto del investigado como de terceros no involucrados en el procedimiento.

[3] Siguiendo los datos de *DataReportal,* "Digital around the Word".

El trabajo se estructura en torno a un análisis comparativo entre las medidas tradicionales de interceptación de comunicaciones telefónicas y telemáticas y las técnicas digitales mencionadas, prestando especial atención a la protección de los derechos fundamentales y a los riesgos del empleo de la tecnología en las técnicas de investigación actuales. Para ello, se estudiarán tanto las disposiciones legales como la jurisprudencia más relevante y las aportaciones doctrinales, así como los recientes desarrollos legislativos en el ámbito europeo.

II. MARCO CONCEPTUAL Y NORMATIVO DE LA INVESTIGACIÓN POLICIAL DIGITAL

1. CONCEPTO DE DILIGENCIAS DE INVESTIGACIÓN TECNOLÓGICAS Y CONCRECIÓN DE LA INTERCEPTACIÓN DE LAS COMUNICACIONES TELEFÓNICAS Y TELEMÁTICAS

Las diligencias de investigación tecnológicas se recogen por primera vez de manera sistemática en la reforma de la Ley de Enjuiciamiento Criminal (en adelante, LECrim) llevada a cabo por la Ley Orgánica 13/2015 de 5 de octubre, para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Esta reforma acoge una serie de medidas que van a restringir en mayor o menor medida los derechos fundamentales, principalmente aquellos recogidos en el artículo 18 de la Constitución Española (CE)[4].

Resulta pertinente comenzar con una aclaración del concepto de diligencias de investigación. Estas medidas se enmarcan en la fase de instrucción o fase sumarial cuya finalidad es comprobar si procede la celebración del juicio y, en su caso, esclarecer los hechos e identificar a los posibles autores del delito[5]. Dentro de esta fase, las diligencias de investigación cumplen la función de recabar la información necesaria para determinar si se ha cometido un hecho delictivo y quién es el presunto

[4] El preámbulo de la Ley Orgánica 13/2015 establece que se unifica la regulación de las medidas de investigación tecnológicas limitativas de los derechos fundamentales recogidos en el artículo 18 de la Constitución.
[5] Artículo 299 LECrim.

autor del mismo[6]. La caracterización de estas diligencias como tecnológicas es señalada por PÉREZ GIL, al mencionar que "en la actualidad la investigación o es tecnológica o no es investigación"[7]. Por lo que sería posible extender la definición general de las diligencias de investigación para incluir a las tecnológicas, ya que este concepto abarca cualquier tipo de medida tendente al esclarecimiento del hecho punible.

Dentro de estas diligencias nos vamos a centrar en la interceptación de las comunicaciones telefónicas y telemáticas, por lo que también es relevante hacer una referencia conceptual sobre estas. Por interceptación de las comunicaciones puede entenderse, tal y como ha indicado la jurisprudencia del Tribunal Supremo como: "una diligencia de investigación, acordada por la autoridad judicial en fase de instrucción, ejecutada bajo el control y supervisión del órgano jurisdiccional competente y acordada con el objeto de captar el contenido de las comunicaciones del sospechoso o de otros aspectos del iter comunicador, con el fin inmediato de investigar un delito, sus circunstancias y autores y con el fin último de aportar al juicio oral materiales

[6] ASENCIO MELLADO, J.M. y FUENTES SORIANO, O., *Derecho procesal penal,* Tirant lo Blanch, Valencia, 1.ª edición, 2019, pág. 107.

[7] PÉREZ GIL, J., "Medidas de investigación tecnológica en el proceso penal español: privacidad vs. eficacia en la persecución", en: BRIGHI, R., PALMIRANI, M. y SÁNCHEZ JORDÁN, M.E (dirs.), *Informatica giuridica e informatica forense al servizio della società della conoscenza. Scritti in onore di Cesare Maioli*. Editorial Aracne, Roma, 2018, pág. 2.

probatorios 'bien frente al imputado, bien frente a otros con los cuales éste se comunique' "[8].

Es decir, es una medida que, al implicar una restricción de derechos fundamentales requiere una resolución judicial motivada que autorice a la Policía Judicial a recabar información relevante para el juicio oral[9].

No hay una distinción en la legislación entre lo que se considera comunicación telefónica y telemática. La jurisprudencia sí que aborda el concepto de intervención de una comunicación telefónica en la Sentencia del Tribunal Supremo de 28 de noviembre de 1994, en la que especifica que se trata de una actividad de control de las comunicaciones entre particulares que implica una restricción del derecho del secreto de las comunicaciones y que debe ser ordenada por una autoridad judicial[10]. Respecto a la comunicación telemática, puede entenderse como la interceptación en tiempo real y sin interrupciones de las comunicaciones[11]. En la Circular 2/2019 de 6 de marzo, de la Fiscalía General del Estado, sobre interceptación de comunicaciones telefónicas y telemáticas[12] se menciona también esta distinción,

[8] Definición textual recogida de la STS 246/1995, de 20 de febrero.

[9] GIMENO SENDRA, J., "La intervención de las comunicaciones telefónicas y electrónicas", *El notario del siglo XXI.* Revista del Colegio Notarial de Madrid, nº. 39, (2011).

[10] Véase STS 2093/1994, de 28 noviembre (núm. Rec. 1149/1993).

[11] CABEZUDO RODRÍGUEZ, N., "Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal", *Boletín del Ministerio de Justicia*, vol. 70, nº 2186, (2016), pág. 29.

[12] FISCALÍA GENERAL DEL ESTADO. Circular de la Fiscalía General del Estado 2/2019, *sobre interceptación de*

poniendo el foco en el medio empleado para realizar la comunicación, de modo que telefónica sería aquella comunicación para la cual se emplee un teléfono y telemática cuando se utilice un sistema informático.

No obstante, aunque exista una distinción teórica entre ambos conceptos, en la práctica sus implicaciones son mínimas y ambas tienen una misma regulación, por lo que no se plantean problemas derivados de su diferenciación[13].

Dentro de esta fase de investigación del delito, y en relación con las diligencias de investigación tecnológicas, es relevante mencionar la expansión del uso de la tecnología en la investigación. La investigación policial digital cobra mayor importancia en una era digital en la que una gran parte de la información se halla en instrumentos tecnológicos. Esto permite mayor facilidad en el acceso a los datos necesarios para la identificación del hecho delictivo y su autor; sin embargo, también facilita la posible afectación de derechos fundamentales[14]. En este contexto, abordaremos dos

comunicaciones telefónicas y telemáticas, de 6 de marzo de 2019. Disponible en: https://www.fiscal.es/documents/20142/12049669/Circular+2_2019%2C+de+6+de+marzo%2C+sobre+interceptaci%C3%B3n+de+comunicaciones+telef%C3%B3nicas+y+telem%C3%A1ticas.pdf/a4d45f8a-a07e-be4b-d8f6-f26c6559127c?t=1739201541483

[13] VARONA JIMÉNEZ, A., "Aspectos relevantes de la interceptación de las comunicaciones telefónicas en el proceso penal español", *Ius Inkarri*, vol. 9, nº 9, (2020), pág. 243.

[14] COLOMER HERNÁNDEZ, I., "Limitaciones en el uso de la información y los datos personales en un proceso penal digital", FREITAS, P. M., (Coord.), *El proceso penal ante una*

técnicas de investigación digital clave para las investigaciones y que generan preocupaciones sobre la privacidad y la protección de derechos: las técnicas de Inteligencia de Fuentes Abiertas (OSINT) y la obtención de direcciones IP.

Una vez aclarado el marco conceptual, es pertinente incidir en el marco normativo que regula esta materia. Este análisis permitirá comprender cómo el ordenamiento jurídico ha abordado la introducción de nuevas diligencias basadas en la tecnología y permitirá la comparación con las concretas técnicas de investigación digital abordadas en el presente trabajo. En este sentido, es clave examinar las disposiciones vigentes, la interpretación jurisprudencial y la dada por la Fiscalía, con el fin de identificar sus limitaciones y desafíos en la práctica de la defensa de los derechos fundamentales.

2. INTERCEPTACIÓN DE LAS COMUNICACIONES TELEFÓNICAS Y TELEMÁTICAS: MARCO NORMATIVO Y JURISPRUDENCIAL.

En este apartado se expone la regulación de la interceptación de las comunicaciones telefónicas y telemáticas, una forma de investigación que cuenta con un marco normativo claro y definido, en contraste con la falta de regulación específica de otras técnicas de investigación digital. A través de la regulación de estas diligencias, se establecen una serie de garantías dirigidas a proteger los derechos fundamentales de los ciudadanos, asegurando que cualquier intervención en este ámbito se realice bajo control judicial y con los

nueva realidad tecnológica europea, Thomson Reuters Aranzadi, Navarra, 2023, págs. 40 y 41.

requisitos legales pertinentes. Sin embargo, en el ámbito de las técnicas de investigación digital que se verán en el siguiente apartado, la ausencia de una regulación precisa puede llegar a suponer una amenaza para los derechos.

Respecto a la interceptación de las comunicaciones telefónicas y telemáticas, la LO 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, se constituye como la principal regulación al introducir una serie de novedades que permiten un avance legislativo para adaptar esta diligencia a la nueva realidad tecnológica presente. Además, se publica la Circular 2/2019 para ofrecer un análisis más detallado de la regulación sobre la interceptación de las comunicaciones telefónicas y telemáticas tras la reforma de la LECrim por la LO 13/2015, la cual se basa en la labor de la jurisprudencia que, durante años, ha ido supliendo las carencias legislativas en materia de diligencias tecnológicas, presentes en la LECrim[15].

La reforma a través de LO incluye cinco medidas de investigación y una serie de disposiciones comunes a ellas. En concreto, la interceptación de las comunicaciones telefónicas y telemáticas se regula en el Capítulo V, "La interceptación de las comunicaciones telefónicas y telemáticas". Este capítulo se inicia con el

[15] ÁLVAREZ MEDIALDEA, A. F., "Cuestiones controvertidas en torno a la diligencia de captación y grabación de las comunicaciones orales mediante la utilización de dispositivos electrónicos. Determinación del concepto de encuentro", *Revista Penal,* nº 51 (2023), pág. 10.

artículo 588 *ter a* LECrim en el que se hace referencia a los requisitos necesarios para que se pueda interceptar una comunicación. Solo se podrá autorizar una interceptación de las comunicaciones telefónicas y telemáticas cuando se esté investigando alguno de los delitos del artículo 579.1 LECrim. Los cuales son: delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión; delitos cometidos en el seno de un grupo u organización criminal y delitos de terrorismo. En cuanto a los delitos conexos, la Circular establece que, si el hallazgo casual está conectado con la prueba matriz, se podría aplicar la diligencia a ese hallazgo, siempre y cuando se mantenga el delito principal que motivó la autorización en un primer momento y excluye la aplicación a delitos imprudentes.

De este modo se respeta el principio de proporcionalidad al restringir el uso de esta diligencia a los supuestos más graves, puesto que se trata de una situación que va a limitar los derechos fundamentales del artículo 18 CE[16].

La Circular especifica que el ámbito de aplicación se limita a aquellas medidas de investigación que afecten a los derechos recogidos en el artículo 18 CE, estos son: el derecho al honor, a la intimidad personal y familiar y a la propia imagen, la inviolabilidad del domicilio y el secreto de las comunicaciones. Y, en particular, aquellas que afecten a datos relacionados con el mensaje en sí, los datos externos de la comunicación, el momento,

[16] LÓPEZ FERIA, A., "Nuevas tecnologías e interceptación de las comunicaciones telefónicas y telemáticas", *Revista Española de Derecho Militar,* nº 111 y 112 (2019), pág. 223.

duración y destino de la comunicación y el acceso a mensajes de texto o SMS no leídos[17].

El ámbito objetivo de los supuestos mencionados anteriormente se establece en el artículo *588 ter b,* se extiende a: la comunicación en sí misma, los datos electrónicos de tráfico o asociados, así como aquellos producidos con independencia de la existencia o no de una determinada comunicación. La Circular aclara que es el Juez quien debe llevar a cabo una delimitación concreta del alcance de la interceptación y establecer si se extiende más allá del contenido concreto de la comunicación alcanzando otros datos asociados. Esta extensión debe estar debidamente justificada conforme a los principios de necesidad, proporcionalidad y excepcionalidad[18].

En relación al ámbito subjetivo, se debe relacionar el dispositivo investigado con su dueño, quien puede adoptar tres formas distintas: investigado, si es el usuario habitual del dispositivo objeto de la diligencia; víctima, cuando su vida o integridad puedan correr grave riesgo[19] y tercero ajeno, en los casos en los que esté actuando como canal para la transmisión de la comunicación, se beneficie de la colaboración con el investigado o su dispositivo esté siendo utilizado por un tercero sin su conocimiento [20]. Asimismo, impone el deber de colaborar con la Administración de Justicia a toda persona o entidad que tenga una vinculación con la comunicación que está siendo investigada, incluyendo a

[17] Véase "Alcance de la medida" de la Circular 2/2019.
[18] Véase "Ámbito objetivo" de la Circular 2/2019.
[19] Artículo 588 *ter b* LECrim.
[20] Artículo 588 *ter c* LECrim.

los prestadores de servicios en el artículo 588 *ter e* LECrim. La Circular clarifica que no es necesario que el terminal esté a nombre del investigado ya que lo que prima es la relación del dispositivo con el usuario y no con el titular de este. Para estos casos en los que no sea el titular será necesario una motivación más detallada de la medida[21].

La solicitud viene regulada en el artículo 588 *ter d* y el artículo 588 *bis b* LECrim y se puede sintetizar en que debe contener: la descripción del hecho objeto de la investigación, la identidad de los afectados por la medida y de los dispositivos a investigar, las razones que la justifican, la extensión de la medida, la unidad investigadora encargada, la forma de ejecución, la duración y la persona responsable de llevar a cabo la medida[22].

De sobremanera, el artículo 588 *bis b* en relación con las disposiciones comunes a la interceptación de las comunicaciones, establece que la solicitud de autorización judicial debe recoger las razones que justifiquen la medida y los indicios de criminalidad, por lo tanto, no es posible solicitar la medida para comprobar de forma general si hay o no un hecho delictivo[23]. Es

[21] Véase "Ámbito subjetivo y afectación de terceros" de la Circular 2/2019.
[22] RAYÓN BALLESTEROS, M. C., "Medidas de investigación tecnológica en el proceso penal la nueva redacción de la Ley de Enjuiciamiento Criminal operada por la Ley Orgánica 13/2015", *Anuario jurídico y económico escurialense,* nº 52 (2019), pág. 185.
[23] ALFONSO RODRÍGUEZ, A. J., "Interceptación de comunicaciones telefónicas, seguridad(es) y garantías procesales", *Ciencia Policial,* nº *182*, pág 117.

necesario que haya indicios serios de criminalidad y no solo suposiciones de que se estuviese cometiendo un delito, tal y como se expresa en la Sentencia del Tribunal Constitucional 49/1999, de 5 de abril[24].

Para garantizar un adecuado control de la medida, se debe acudir a lo dispuesto en el artículo *588 bis g* en materia de disposiciones comunes y al artículo *588 ter f* LECrim. Estos artículos establecen el deber de información de la Policía Judicial al Juez de Instrucción, las formalidades que debe tener la resolución judicial habilitante, la obligación de poner a disposición del Juez dos soportes digitales: uno con la transcripción y otro con las grabaciones, etc. La Circular señala que la LECrim no recoge el momento en que se debe practicar la prueba y remite a la jurisprudencia. En concreto, la Sentencia del Tribunal Supremo 513/2010, de 2 de junio, indica que si las partes lo solicitan se deberá escuchar en el momento del juicio oral[25].

En cuanto a la duración de la medida, los artículos 588 *ter g y ter h* LECrim establecen que debe ser de máximo tres meses, prorrogables por periodos sucesivos de tres meses hasta un máximo de dieciocho meses computables desde la fecha de autorización judicial y en relación con cada investigado. En la Circular se alude al principio de proporcionalidad y establece que se deberá ir incrementando la motivación con cada prórroga y que no basta con una remisión a la autorización por el plazo

[24] Véase STC 49/1999, de 5 de abril.
[25] Véase STS 513/2010, de 2 de junio

inicial, tal y como se especifica en la Sentencia del Tribunal Constitucional 181/1995 de 11 de diciembre[26].

Tras la finalización de las medidas y una vez alzado el secreto de la medida, las partes tienen derecho a conocer el resultado de las investigaciones realizadas, por lo que se les debe de entregar una copia de las grabaciones y de las transcripciones realizadas sin incluir aquellos datos sobre la vida íntima de las personas, lo cual debe ser señalado por el Juez[27]. De igual manera, la circular indica el derecho de terceros afectados a conocer sobre la intervención de sus comunicaciones, siempre y cuando la notificación no resulte imposible, no requiera un esfuerzo desproporcionado o pueda perjudicar a investigaciones futuras. Posteriormente, se debería proceder a la destrucción de los registros tal y como establece el artículo 588 *bis k.*

Por último, en lo que respecta a la incorporación al proceso de datos de tráfico, cabe señalar que estos serán abordados con mayor detenimiento posteriormente. En lo que aquí incumbe, es preciso destacar el artículo 588 *ter j* LECrim que reitera que la incorporación de estos datos requiere de autorización judicial. Asimismo, el asunto de las direcciones IP será explicado en capítulos posteriores y en este sentido el artículo 588 *ter k* LECrim menciona que la Policía Judicial puede solicitar al Juez de Instrucción el requerimiento a los prestadores de servicios para que estos les faciliten los datos necesarios para la identificación del dispositivo

[26] Véase STC 181/1995, de 11 de diciembre.
[27] BUENO DE MATA, F., BUJOSA VADELL, L. (pr.), *Las diligencias de investigación penal en la cuarta revolución industrial. Principios teóricos y problemas prácticos,* Thomson Reuters Aranzadi, Navarra, 2019, 1.ª edición, pág. 80.

y del sospechoso. La Circular explica que la Policía Judicial no va a necesitar autorización judicial para determinar la dirección IP si puede hacerlo valiéndose de sus propios medios. Sin embargo, será necesario autorización judicial para vincular esa dirección IP con un equipo o dispositivo concreto y con el usuario de este[28].

En definitiva, la reforma introducida por la LO 13/2015 y los detalles recogidos en la Circular 2/2019, buscan establecer un marco normativo que garantice la máxima protección de los derechos fundamentales de los investigados. Sin embargo, se trata de una situación delicada ya que no siempre resulta sencillo lograr un equilibrio entre la necesidad de llevar a cabo una investigación eficaz y el respeto a los derechos de los investigados. Esta fricción se ve especialmente reflejada en el uso de técnicas como la Inteligencia de Fuentes Abiertas o la obtención de direcciones IP, las cuales, a pesar de ser herramientas valiosas para el esclarecimiento de delitos, pueden afectar directamente a los derechos fundamentales de las personas implicadas por la falta de un encaje preciso en la regulación anteriormente expuesta. Esta tensión y afectación de derechos se irán mostrando a lo largo del presente trabajo, evidenciando los desafíos que presenta la aplicación de estas medidas.

III. INVESTIGACIÓN POLICIAL DIGITAL

Dentro del marco de las relaciones de la investigación policial digital con los derechos fundamentales, es

[28] Véase "Incorporación al proceso de datos de tráfico o identificación" de la Circular 2/2019.

pertinente analizar los dos métodos de investigación digital anteriormente señalados y cuyas implicaciones son de especial relevancia para este trabajo: el empleo de técnicas de Inteligencia de Fuentes Abiertas (OSINT) y la obtención de direcciones IP. Estas herramientas se caracterizan por la obtención de datos sin necesidad de autorización judicial, puesto que se considera que no afectan de forma significativa a los derechos fundamentales del artículo 18 CE. Sin embargo, es esta falta de autorización la que provoca una disminución de las garantías y de la protección de estos derechos, lo que plantea importantes desafíos en su salvaguarda. Ambas técnicas representan el dilema clásico entre eficacia en la investigación criminal y la protección de los derechos fundamentales, un conflicto que se enfatiza aún más por el menor nivel de regulación que poseen frente a otros métodos de investigación.

En una sociedad marcada por lo digital, donde la mayoría de las interacciones y comunicaciones se realizan en línea, la privacidad se traslada a un entorno virtual, por lo que el acceso a datos alojados en Internet se convierte en un nuevo peligro para los derechos fundamentales. La digitalización ha transformado los conceptos de intimidad y secreto de las comunicaciones, obligando a replantear los límites de la vigilancia policial y la regulación de las principales técnicas que actúan en este entorno digital: el OSINT y las direcciones IP.

El OSINT se refiere a las técnicas de recopilación, procesamiento y correlación de información obtenida de

fuentes públicas[29], como redes sociales, foros y otros recursos en línea.

Por otro lado, las direcciones IP son números únicos asignados a cada dispositivo conectado a una red que sirve para identificarlos[30]. Con las técnicas OSINT, la Policía puede aprovechar la información pública disponible en diversas plataformas y correlacionarla con la dirección IP asociada a un sospechoso.

Por ello, la combinación de estas dos metodologías amplía significativamente el alcance de la investigación digital, pero también plantea desafíos críticos en materia de protección de la intimidad y otros derechos fundamentales[31].

[29] LENOIR-GRAND PONS, R., "Análisis de riesgo, prevención y comunicación en la gestión de crisis", MOLINER GONZÁLEZ, J. A., GONZÁLEZ-RABANAL, M. C. (Dirs.), *Seguridad, control de fronteras y derechos humanos. Gestión pública de las crisis sociales,* Dykinson, Madrid, 2022, pág. 242.

[30] BARRIO ANDRÉS, M., *Derecho Público e Internet: la actividad administrativa de regulación de la Red*, Instituto Nacional de Administración Pública (INAP), Madrid, 2017, 1ª edición, pág. 78.

[31] ORTIZ PRADILLO, J. C., "Dispositivos o medios técnicos de seguimiento y localización en el proceso penal", RODRÍGUEZ LAINZ, J. L. (Dir.), *Diligencias de investigación tecnológica,* Cuadernos digitales de formación nº 5, Consejo General del Poder Judicial, Madrid, 2018, pág. 50.

1. INTELIGENCIA DE FUENTES ABIERTAS U "OPEN SOURCE INTELLIGENCE" (OSINT).

A) *Concepto del OSINT y su relación con la interceptación de las comunicaciones telefónicas y telemáticas.*

La Inteligencia de Fuentes Abiertas u "Open Source Intelligence" (OSINT) puede entenderse como la recolección, procesamiento y correlación de información pública obtenida a través de fuentes abiertas como las redes sociales, foros, blogs, datos comerciales, etc.[32] Esta información puede utilizarse para obtener datos sobre los sujetos de una investigación. Se trata de un mecanismo muy eficiente por el bajo coste de los recursos a utilizar, además de que se vale de una gran cantidad de información actualizada que ofrecen estas fuentes abiertas. Sin embargo, este amplio abanico de datos puede convertirse en un problema a la hora de discernir entre aquellos que son relevantes de los que no[33].

Dentro de OSINT pueden encontrarse distintas variantes en función de la fuente de la que provenga la información, tales como: SIGINT, si proviene de señales de satélites públicos, HUMINT, si procede de entrevistas u observación directa, IMINT, si se utilizan imágenes de

[32] PASTOR-GALINDO, J., NESPOLI, P., MÁRMOL, F. G., PÉREZ, G. M, "The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends", *IEEE access,* vol. 8 (2020), pág. 10282.

[33] ROJO TORRES, J. D., "OsiNET desarrollo de una herramienta de integración OSINT", *Alcalibe: Revista Centro Asociado a la UNED Ciudad de la Cerámica,* nº 23 (2023), págs. 182 y 183.

espacios públicos o SOCMINT, si procede de redes sociales[34].

El marco legal aplicable a OSINT teniendo en cuenta que se trata de una medida de investigación tecnológica y que puede aplicarse a aquella información derivada de una diligencia de investigación, es la Ley de Enjuiciamiento Criminal[35]. Sin embargo, a tenor de lo explicado con anterioridad sobre la interceptación de las comunicaciones telefónicas y telemáticas, se puede concluir que el OSINT no es propiamente una diligencia de este tipo, puesto que no requiere una intervención de un medio de comunicación, sino que la investigación se realiza a través de fuentes públicas accesibles para cualquier persona[36]. Es decir, la interceptación accede directamente a comunicaciones privadas (llamadas, correos, mensajes, etc.) lo que proporciona una información más directa y confidencial por no ser posible el acceso del público general a ella, mientras que OSINT permite obtener datos de manera pasiva, aprovechando la huella digital pública del investigado.

---

[34] BUENO DE MATA, F., "Técnicas de ciberinteligencia aplicables a la investigación de delitos de odio en redes abiertas: reflexiones críticas", en AGUILAR CÁRCELES, M. M., SOTO CASTRO, J. E., VINAGRE GONZÁLEZ, A. M., (Dirs.), *Delitos de odio. Un abordaje multidisciplinar*, J.B. Bosch, Barcelona, 2023, pág. 62.

[35] BUENO DE MATA, F., *Investigación y prueba de delitos de odio en redes sociales técnicas OSINT e inteligencia policial,* Tirant lo Blanch, Valencia, 2023, 1ª Edición, pág. 124.

[36] TORO-ALVAREZ M. M., BONILLA-DUITAMA M. L., PARADA JAIMES W. D., "Investigación del Cibercrimen y de los Delitos Informáticos Utilizando Inteligencia de Fuentes Abiertas de Información (OSINT)", *Researchgate,* (2018), pág. 4.

Por lo tanto, pese a tener el mismo objetivo de obtener información sobre los hechos y personas investigadas, la interceptación de comunicaciones telefónicas y telemáticas y el OSINT utilizan medios diferentes que hacen que su regulación varíe sustancialmente.

Según la LECrim, la interceptación de comunicaciones telefónicas y telemáticas necesita de autorización judicial por entenderse que afecta a derechos fundamentales[37]. Sin embargo, la propia ley contempla una serie de medidas de investigación que no precisan de dicha autorización judicial al no vulnerar, en principio, estos derechos fundamentales. Entre estas medidas, se encuentra la investigación a través de OSINT[38], que, aunque se basa en fuentes abiertas, en la práctica puede suponer una intromisión en la privacidad si no se lleva a cabo adecuadamente.

De este modo, las protecciones que la LECrim ofrece a los derechos relacionados con la interceptación de las comunicaciones no serían aplicables a la obtención de información mediante OSINT, lo que implica menores garantías, así como una posible vulneración de los derechos fundamentales, especialmente cuando la información obtenida permite reconstruir aspectos íntimos de la vida del investigado o de terceros.

B) Derechos fundamentales afectados

Pese a que las técnicas OSINT accedan solo a información pública, la gran cantidad de datos

[37] Artículo 588 *bis a* LECrim.
[38] MARTÍNEZ GALINDO, G., "Problemática jurídica de la prueba digital y sus implicaciones en los principios penales", *Revista Electrónica de Ciencia Penal y Criminología,* nº 24-23 (2022), pág. 12.

recopilados y su combinación pueden ofrecer una visión detallada sobre la vida privada de las personas. Esta práctica puede permitir reconstruir aspectos íntimos, como rutinas, relaciones personales o ideologías, lo que podría afectar de igual o mayor manera que otros medios más intrusivos como la interceptación de las comunicaciones. Esto se debe precisamente a la falta de una regulación específica y de un control judicial previo que garantice la proporcionalidad entre la investigación y la protección de los derechos fundamentales recogidos en la Constitución[39].

En relación con los derechos recogidos en el artículo 18 CE, en concreto, el apartado primero sobre el derecho a la intimidad personal y familiar, se puede observar como este derecho es afectado por la investigación mediante OSINT. Aunque la información que se obtiene a través de este mecanismo es pública, el sujeto que la ha compartido no ha otorgado su consentimiento para su recopilación y análisis. Estos datos que el investigado publica no han sido difundidos con la intención de ser objeto de un examen masivo y exhaustivo que permita elaborar perfiles detallados sobre su vida personal.

Tal y como expone EDUARDO BERTONI, se puede argumentar que la información vertida en redes sociales es publicada tras la lectura y aceptación de los "términos y condiciones" de las plataformas, lo que implica que los

[39] En el mismo sentido, MONTE, M., SÁNCHEZ. S.I., "Tensiones constitucionales entre el derecho a la intimidad y el ciberpatrullaje en la investigación criminal. Análisis del Protocolo General para la Prevención Policial del Delito con Uso de Fuentes Digitales Abiertas", *Revista Pensamiento Penal,* (2021), pág. 8.

usuarios son conscientes de que su contenido es de libre acceso y, por lo tanto, no habría expectativas de privacidad sobre ello. No obstante, esto presupone que los usuarios han comprendido lo que implica la aceptación de estos términos, lo que no siempre ocurre. Además, no todos los datos que almacenan las redes sociales son aquellos que se han compartido voluntariamente. Existen datos tales como la geolocalización, la fecha o los dispositivos utilizados que no son directamente publicados por el usuario y que, sin embargo, pueden ser analizados por mecanismos como OSINT[40]. Información como el uso de aplicaciones de terceros, interacciones con anuncios, comportamiento de clics o el tiempo de pantalla, también pueden ser recopiladas y analizadas sin que los usuarios de las aplicaciones que recogen estos datos sean conscientes de su existencia[41].

Además, la Sentencia del Tribunal Constitucional 27/2020, de 24 de febrero, señala que el uso extendido de la tecnología ha provocado una mayor afectación de los derechos fundamentales al honor, a la intimidad, a la propia imagen y a la protección de datos de carácter personal[42]. Del mismo modo, la sentencia advierte que las redes sociales pueden implicar una pérdida de control sobre la información que el usuario comparte, lo que

[40] BERTONI, E., "Las prácticas OSINT, ¿son amigas o enemigas de los derechos humanos?", *CELE Research,* nº 58 (2023), pág. 15.
[41] HULSEN, L. TEN., "Open Sourcing Evidence from the Internet- the Protection of Privacy in Civilian Criminal Investigations Using Osint (Open-Source Intelligence)", *Amsterdam Law Forum*, vol. 12, nº 2 (2020), pág. 36.
[42] Véase STC 27/2020, de 24 de febrero.

facilita que terceros puedan utilizarla con fines distintos a los que motivaron su publicación original.

Esta sentencia incide igualmente en la posibilidad de que un usuario publique información sobre otro sin su consentimiento. Cuando se difunde un vídeo o una imagen en la que aparece el investigado, pero esta ha sido publicada por otra persona, su identidad puede quedar expuesta en Internet sin su autorización e incluso sin que él sea consciente de dicha publicación. Por tanto, el empleo de técnicas OSINT sobre este tipo de datos no publicados directamente por el investigado, puede agravar más aun la vulneración de sus derechos al no haber hecho pública él mismo esa información**.**

Asimismo, la recopilación de datos mediante OSINT, puede afectar no solo al investigado, sino también a terceros ajenos a la investigación cuya información se haya obtenido incidentalmente, sin que exista una regulación clara sobre el procesamiento y conservación de esos datos. A diferencia de la interceptación de comunicaciones telefónicas y telemáticas, en la que se debe cumplir con procedimientos detallados sobre la conservación de estos datos y su uso en el procedimiento judicial, debiéndose eliminar aspectos de la vida íntima de las personas que pudieron haber quedado reflejados en ella[43], la investigación a través de OSINT carece de un mecanismo de control análogo. Por lo tanto, la expansión del análisis de datos a personas no implicadas con la investigación puede vulnerar el derecho a la intimidad y a la protección de datos, lo que también entra en conflicto con el principio de

[43] Artículo 588 *ter i* LECrim.

proporcionalidad[44]. Este principio exige que las medidas adoptadas sean adecuadas, necesarias y proporcionadas a los fines que se persiguen, evitando que se vulneren derechos fundamentales de manera injustificada.

En este sentido, el voto particular emitido por Excmo. Sr. Magistrado D. Manuel Marchena Gómez a la Sentencia recaída en el recurso de Casación núm. 11347/2011, destaca que los avances tecnológicos en las comunicaciones telefónicas y telemáticas deberían exigir una interpretación más estricta y actualizada del deber de motivación judicial y del principio de proporcionalidad. El Juez debería de valorar, ante la gran cantidad de información disponible, cuál es realmente necesaria para la investigación[45]. Esta reflexión refuerza la idea de que la recopilación de datos mediante OSINT, al implicar la injerencia sobre información personal, debería estar acompañada de mayores garantías legales. La proporcionalidad, por tanto, exige que los datos recolectados sean imprescindibles para la investigación. Así, si para la interceptación de comunicaciones es necesario discernir la información relevante de la que no lo es, la investigación mediante OSINT debería cumplir con este mismo requisito, puesto que, aunque no se trate formalmente de una intervención de las comunicaciones, afecta en esencia al mismo contenido protegido por los derechos fundamentales.

[44] BARONA VILAR, S., "Justicia con algoritmos e inteligencia artificial, ¿acuerpando garantías y derechos procesales o liquidándolos?", *Derechos y Libertades,* nº 51, Época II (2024), pág. 104.
[45] Véase STS 15/2012, 20 de enero.

De sobremanera, el artículo 588 ter f LECrim establece un procedimiento minucioso de control de la autenticidad e integridad de la información, aspecto que no sucede en la averiguación de datos a través de OSINT, lo cual puede conllevar problemas en cuanto a la fiabilidad de los datos obtenidos. La información de fuentes abiertas puede ser modificada, utilizando una diferente etiqueta de geolocalización, etiquetando a personas que no se encuentran en la imagen o editando las fotos o vídeos con *Photoshop,* lo cual puede dar pistas falsas si no se analizan bien los recursos disponibles[46].

La ausencia de un control judicial estricto sobre el OSINT no solo permite la recopilación y uso de datos sin salvaguardias, sino que también facilita que el uso de tecnologías como la Inteligencia Artificial, sin una supervisión adecuada, pueda generar resultados sesgados que afecten la imparcialidad del proceso de investigación.

Por ello, la posibilidad de incurrir en sesgos algorítmicos[47] se constituye como un riesgo sobre los derechos. La información obtenida a partir de fuentes abiertas analizada de manera aislada puede no conllevar ninguna connotación y ser neutral, sin embargo, una vez

[46] HULSEN, L. TEN., Op. cit., pág. 25.
[47] BARONA VILAR, S., "El algoritmo en la prueba y en la decisión judicial: ¿instrumental o funcional?", BUSTAMANTE RÚA, M. M., HENAO OCHOA, A. DEL P., RAMÍREZ CARVAJAL, D. M. (Coords.), *La justicia en la era de la revolución tecnológica,* Institución Universitaria de Envigado, Envigado, 2023, pág. 20.

recopilada y analizada en conjunto puede crear un perfil sesgado del investigado. Si el procesamiento de datos en OSINT se realiza utilizando Inteligencia Artificial (IA) se puede caer en las tendencias de sesgos algorítmicos, entendidos estos según FERRANTE como "sistemas cuyas predicciones benefician sistemáticamente a un grupo de individuos frente a otro, resultando así injustas o desiguales"[48]. Estos sesgos pueden proceder del proceso de entrenamiento o del diseño de la Inteligencia Artificial, en el que se utilizan datos históricos que pueden contener sesgos derivados de la sociedad, la cultura o decisiones pasadas. Por lo que, si un sistema de Inteligencia Artificial utilizado para el análisis de OSINT se entrena con datos que históricamente han reflejado discriminación, los resultados que genere el sistema pueden replicar esos sesgos[49], los cuales, a su vez, pueden influenciar la actividad del investigador y conllevar a la vulneración del principio de igualdad y no discriminación recogido en el artículo 14 CE, así como el derecho a un juicio con todas las garantías del artículo 24.2 CE en el que no se vea afectada la imparcialidad del Juez.

No se debe ignorar la distinción entre el concepto de dato abierto o cerrado dentro del entorno digital, tal y como menciona BUENO DE MATA[50], ya que puede afectar al

[48] FERRANTE, E., "Inteligencia artificial y sesgos algorítmicos. ¿Por qué deberían importarnos?", *Nueva Sociedad,* nº 294 (2021), pág. 29.
[49] MATTEO PASQUINELLI, V. J., "El Nooscopio de manifiesto. La inteligencia artificial como instrumento de extractivismo del conocimiento.", *La Fuga,* nº 25 (2021), pág. 3.
[50] BUENO DE MATA, F., Op. cit., pág 133.

derecho a la intimidad y al secreto de las comunicaciones del artículo 18 CE.

Para ello, es necesario abordar el dilema de si la información obtenida a través de OSINT puede considerarse realmente pública. Algunos autores señalan que los datos compartidos en redes sociales tienen una "doble naturaleza", por una parte, se genera una sensación de privacidad para los usuarios y por otra, dicha información se encuentra en espacios públicos[51]. Además, existe cierta ambigüedad en la distinción entre información pública y privada, ya que dentro de cada categoría pueden incluirse datos con características de ambas. Por esta razón, mucha de la información publicada en redes no puede clasificarse estrictamente como privada, pero tampoco debería considerarse completamente pública[52].

En esta línea, el Tribunal Europeo de Derechos Humanos (TEDH), en el caso *Rotaru contra Rumanía*[53] sostuvo que cuando los datos públicos se recogen y memorizan de manera sistemática pueden entrar dentro del ámbito de la vida privada y suponer una injerencia en los derechos. De manera similar, en el caso *Segerstedt-Wiberg contra Suecia*[54], el Tribunal afirmó que correspondía a la vida

[51] VRIST RØNN, K., OBELITZ SØE, S., "Is social media intelligence private? Privacy in public and the nature of social media intelligence", *Intelligence and National Security*, vol. 34, nº 3 (2019), pág. 366.
[52] MONTE, M., SÁNCHEZ. S.I., Op. cit., pág. 9.
[53] Véase caso Rotaru contra Rumanía, STEDH de 4 de mayo de 2000, Sentencia 28341/95.
[54] Véase caso Segerstedt-Wiberg contra Suecia, STEDH de 6 de junio de 2006, Sentencia 62332/00.

privada aquella información que siendo pública había sido recopilada y almacenada sistemáticamente.

Esto refuerza la idea de que las técnicas OSINT pueden injerir en los derechos de privacidad, en concreto, el derecho a la intimidad personal y familiar del artículo 18 CE. Por lo que, la obtención y procesamiento de información a partir de fuentes abiertas debería estar sujeta a autorización judicial[55] y a un mayor control, de manera similar a lo exigido para la interceptación de comunicaciones telefónicas y telemáticas.

OSINT también puede entrar en conflicto con el derecho fundamental al secreto de las comunicaciones si se accede conversaciones mantenidas en redes sociales. Entendido este derecho por el Tribunal Constitucional como la garantía de los interlocutores a la confidencialidad de la comunicación, comprendiendo tanto la comunicación misma como el contenido y los datos externos y con independencia del carácter público o privado del medio de la transmisión[56].

Aunque las plataformas en las que se comparten los mensajes sean de acceso público, pueden contener espacios cerrados, como grupos privados que requieren invitación o aprobación para participar. Además, los mensajes vertidos en estos chats no deben analizarse en un contexto diferente al mismo, ya que pueden perder su significado original[57]. En estos casos, la diferencia con

[55] En este sentido, MILLETT, E., "Open-Source Intelligence, Armed Conflict, and the Rights to Privacy and Data Protection", *Security and Human Rights Monitor,* (2023), pág. 10.
[56] Véase STC 123/2002, de 20 de mayo.
[57] EIJKMAN, Q., WEGGEMANS, D., "Open source intelligence and privacy dilemmas Is it time to reassess state

una interceptación de las comunicaciones telefónicas y telemáticas se reduce aún más, ya que implica una mayor intromisión del investigador en la vida privada del investigado y supone una vuelta al dilema sobre los límites entre la información pública y privada.

En resumen, las técnicas OSINT, aunque se basan en la recopilación de información pública, pueden tener una serie de injerencias significativas sobre los derechos fundamentales. Estas presentan varios riesgos para la privacidad, como la falta de consentimiento para el uso de datos personales en investigaciones policiales, la recopilación de datos no publicados voluntariamente, la fiabilidad de los datos, los sesgos algorítmicos o el dilema entre lo público y lo privado. Todo esto subraya la necesidad de una regulación más estricta para proteger los derechos fundamentales, sin olvidar que el uso de OSINT sigue siendo una herramienta valiosa para los investigadores, que permite obtener información relevante de manera eficiente, contribuyendo a la resolución de casos complejos[58].

2. LAS DIRECCIONES IP

A) Concepto de direcciones IP y encuadre normativo.

Las direcciones IP conforman otra parte esencial de la investigación digital por su capacidad para identificar dispositivos y rastrear actividades en la red y lo que esto

accountability?", *Security and Human Rights*, vol. 23 (2013), pág 7.

[58] LANDE, D., SHNURKO-TABAKOVA, E., "OSINT as a part of cyber defense system", *Theoretical and Applied Cybersecurity*, vol. 1, nº 1 (2019), pág. 103.

implica para los derechos fundamentales del artículo 18 CE. Estas pueden ser entendidas como el número de identificación de un dispositivo conectado a una red. Este número es único para cada equipo y su función es la de identificar un dispositivo conectado en la red[59]. Su transmisión se realiza a través del Protocolo TCP/IP, por el cual cada dispositivo se identifica con una dirección IP[60].

Dentro de la regulación de la interceptación de las comunicaciones telefónicas y telemáticas, se hace referencia a las direcciones IP en los artículos 588 *ter k* a 588 *ter m* LECrim. Como hemos visto anteriormente, la regla general que establece esta regulación es la necesidad previa de autorización judicial para la intervención de estas comunicaciones. Por lo tanto, se debe diferenciar dos conceptos para determinar el alcance de esta norma: datos de tráfico y datos de abonado.

En toda comunicación telemática, además del mensaje en sí, se generan una serie de datos adicionales. Entre estos datos se hallan aquellos que brindan información sobre el origen, destino y ruta del mensaje; estos son los conocidos como datos de tráfico[61]. Por otro lado, los

[59] PALOP BELLOCH, M., "Las medidas de investigación tecnológica", *Justicia: Revista de derecho procesal,* nº 2 (2017), pág. 467.

[60] LÓPEZ JIMÉNEZ, R., *Victimización sexual y nuevas tecnologías: desafíos probatorios,* Dykinson, Madrid, 2021, 1ª edición, pág. 66.

[61] CALVO LÓPEZ, D., "Capacidades de actuación del ministerio fiscal y la policía judicial tras la reforma procesal operada por la ley orgánica 13/2015: en especial la obtención de direcciones IP y numeraciones IMEI e IMSI (los apartados k)

datos de abonado son la información almacenada por los proveedores de servicios con el objetivo de garantizar la prestación, facturación y cumplimiento de las condiciones contractuales[62]. Estos datos pueden incluir el nombre, dirección, número de teléfono, correo electrónico y otros elementos identificativos del usuario.

Ambos conceptos son definidos en el Convenio de Ciberdelincuencia del Consejo de Europa de Budapest del 23 de noviembre de 2001. Por datos de tráfico entiende "todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indique el origen, destino, ruta, hora, fecha, tamaño, duración o tipo de servicio subyacente" y, por datos de abonado "toda información, en forma de datos informáticos o de cualquier otra forma, que posea un proveedor de servicios y esté relacionada con los abonados a dichos servicios, excluidos los datos sobre el tráfico o sobre el contenido, y que permita determinar: a) El tipo de servicio de comunicaciones utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio; b) la identidad, la dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso o información sobre facturación y pago que se encuentre disponible sobre la base de un contrato o de un acuerdo de prestación de servicios; c) cualquier otra información relativa al lugar en que se encuentren los equipos de comunicaciones, disponible

a m) del art. 588 ter de la LECRIM)", *Jornadas de Especialistas celebradas en el Centro de Estudios Jurídicos de Madrid*, 16 y 17 febrero de 2017, pág. 7.

[62] CALVO LÓPEZ, D., Id.

sobre la base de un contrato o de un acuerdo de servicios"[63].

Los datos de tráfico, como se pudo comprobar en el análisis de la legislación sobre la interceptación, forman parte del contenido del mensaje según la Ley de Enjuiciamiento Criminal y, por ello, para su obtención y análisis debe mediar una autorización judicial.

Esto se refleja en el artículo 588 *ter b* LECrim al extender el ámbito objetivo de aplicación al "contenido de las comunicaciones y a los datos electrónicos de tráfico o asociados al proceso de comunicación".

Sin embargo, la normativa no hace referencia a los datos de abonado, por lo que estos podrían ser obtenidos sin necesidad de autorización judicial al amparo del artículo 588 *ter m* LECrim, que permite a la Policía Judicial obtener los datos identificativos directamente de los prestadores de servicios.

Este artículo también les permite obtener la dirección IP de una comunicación cuando se trata de un dato público de la Red. De este modo, no solo se puede obtener el número de dirección IP sin mayor información, sino que también es posible vincular este número a un usuario a través de los datos disponibles públicamente, tal y como indica el Informe de la Agencia Española de Protección de Datos (AEPD) "en muchos casos existe la posibilidad de relacionar la dirección IP del usuario con otros datos

[63] Convenio de Ciberdelincuencia del Consejo de Europa de Budapest, 23 de noviembre de 2001.

de carácter personal, de acceso público o no, que permitan identificarlo"[64].

Es precisamente esto lo que puede conllevar problemas a la hora de respetar los derechos fundamentales y lo que será abordado a continuación.

B) Derechos fundamentales afectados y problemas de aplicación

La jurisprudencia hasta ahora ha sido clara en lo que respecta a las injerencias en los derechos fundamentales del secreto de las comunicaciones y el derecho a la intimidad por parte de la obtención de direcciones IP sin autorización judicial. El Tribunal Supremo considera que la Policía se limita a obtener una información que el usuario ha introducido en la red y, por tanto, se admite su adquisición sin autorización[65].

De este modo, volvemos al debate sobre si cierta información introducida en la red se hace con el conocimiento y consentimiento del usuario. La obtención de una dirección IP por la Policía Judicial, utilizando sus propios medios y valiéndose de la información pública en la red para rastrear una actividad delictiva o vincular un dispositivo con dicha actividad, podría vulnerar el ámbito de privacidad del usuario y suponer una injerencia en el derecho fundamental a la intimidad personal y familiar, protegido por el artículo 18 CE. Si tomamos en cuenta que el usuario promedio no es consciente de lo que es una dirección IP ni de las implicaciones que esta

[64] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Informe 327/2003", (2003). Disponible en: https://www.aepd.es/documento/2003-0327.pdf
[65] Véase STS 1932/2008, de 9 de mayo.

conlleva[66], suponer que ha dado su consentimiento para que esa información sobre su actividad en la red se haga pública no sería del todo acertado. El argumento de que ha precedido un consentimiento para que esa información sea pública pasa por alto el hecho de que la mayoría de las personas no dedica el tiempo necesario para leer y entender las políticas de los proveedores de servicios[67].

Esta idea es tomada en cuenta por la Corte Suprema de los Estados Unidos. La Corte evalúa el tipo de tecnología utilizada en la investigación y si es razonable suponer que un ciudadano ha comprendido el alcance de su privacidad con respecto a esta, para así determinar si se ha violado su derecho a la intimidad o no, y si es necesario obtener una autorización judicial para usar esa tecnología en la investigación[68].

[66] En la misma línea, un estudio en el marco de la 35ª Conferencia Internacional de Ciencias del Sistema de Hawái demuestra que hay una asimetría de información entre los usuarios y los proveedores de servicios en línea. FRIEDMAN B., FELTEN E., y HOWE, D.C, "Informed Consent in the Mozilla Browser: Implementing Value-Sensitive Design", *Proceedings of the 35th Hawaii International Conference on System Sciences,* vol. 8 (2002), pág. 1.

[67] BASHIR, M., HAYES, C., LAMBERT, A. D., KESAN, J. P., "Online privacy and informed consent: The dilemma of information asymmetry" *Proceedings of the Association for Information Science and Technology*, vol. 52, nº 1 (2015), pág. 2.

[68] ORTIZ PRADILLO, J. C., "La investigación del delito en la era digital. Los derechos fundamentales frente a las nuevas medidas tecnológicas de investigación", *Estudios de Progreso, Fundación Alternativas,* nº 72 (2013), pág. 19.

La falta de comprensión de los usuarios sobre la naturaleza de sus datos en línea pone en evidencia una laguna importante en la protección de la privacidad y la intimidad personal. Es crucial que las autoridades, incluidos los proveedores de servicios, consideren esta falta de conocimiento al utilizar información como las direcciones IP para investigaciones. La privacidad de los usuarios no debe verse comprometida solo porque se haya aceptado un acuerdo sin leer las condiciones.

La obtención de la dirección IP sin autorización judicial basada en el artículo 588 *ter m* LECrim también presenta problemas sobre su implicación sobre los derechos fundamentales. Dado que la dirección IP es la misma tanto si la policía no la obtiene por sus propios medios y requiere de autorización judicial[69] como si la adquiere directamente de los prestadores de servicios sin autorización judicial, no queda clara la distinción entre ambos supuestos. A pesar de que la injerencia sobre la privacidad del usuario es la misma, la protección de su derecho a la intimidad varía según el caso[70].

En relación con los datos de abonado, estos no están considerados dentro del ámbito de protección de los derechos fundamentales, lo que permite su obtención sin autorización judicial. No obstante, su obtención y análisis conjunto puede resultar también peligroso para el derecho a la intimidad personal**.** Estos datos, que incluyen información detallada sobre los servicios

[69] Artículo 588 *ter k* LECrim
[70] RICHARD GONZÁLEZ, M., "Conductas susceptibles de ser intervenidas por medidas de investigación electrónica. Presupuestos para su autorización"**,** *Diario La Ley*, nº 8808 (2016), pág. 6.

utilizados, la identidad del abonado, e incluso los números de acceso y detalles de facturación, permiten crear perfiles sumamente detallados de los usuarios[71]. Este perfil, que podría revelar aspectos privados de la vida de una persona, se construye sin su conocimiento explícito ni su consentimiento informado.

En una línea similar, los jueces PERALTA GUTIÉRREZ y AGUIRRE ALLENDE al analizar la postura del Tribunal de Justicia de la Unión Europea respecto al acceso a los datos de abonado durante la instrucción penal, llegan a la conclusión de que la facultad de recabar sin autorización judicial datos tales como la identidad de un abonado contradicen al Derecho de la Unión[72]. En la Sentencia *Tele2 Sverige AB* contra *Post- och telestyrelsen y Secretary of State for the Home Department* contra *Tom Watson* y otros[73], el Tribunal de Justicia declaró que es necesario un control previo por un órgano jurisdiccional para el acceso y uso de estos datos. Por tanto, dado que estos datos pueden influir directamente en la privacidad, su tratamiento debería ser equiparado al de los datos de tráfico y estar sujetos a la misma regulación y control judicial o bien constar de manera explícita y clara en la información que consienten los usuarios de los prestadores de servicios.

[71] DAMJAN, M., "The protection of privacy of the IP address in Slovenia", *Law, Identity and Values,* vol. 2 (2023), pág 28.
[72] PERALTA GUTIÉRREZ, A., AGUIRRE ALLENDE, P., "El TJUE y el acceso a los datos de abonado en el seno de la instrucción penal", *Diario la Ley,* nº 9420 (2019), pág. 7.
[73] STJUE *Tele2 Sverige AB* contra *post-och telestyrelsen y Secretary of State for the Home Department* contra *Tom Watson* y otros. ECLI**:** ECLI:EU:C: 2016:970

A pesar de que las direcciones IP son una herramienta clave para rastrear actividades en línea, su utilización plantea importantes cuestiones sobre la privacidad y los derechos fundamentales de los usuarios. La obtención de esta información sin el debido proceso puede comprometer la integridad del procedimiento judicial, afectando a los derechos de defensa de los imputados. Por lo tanto, es crucial examinar cómo estos problemas pueden influir en el desarrollo y la legitimidad de los procedimientos judiciales.

Por otro lado, en relación con la identificación del usuario tras la dirección IP, surge un dilema que merece un análisis detallado. Las direcciones IP presentan una serie de problemas de aplicación que pueden afectar, en última instancia, a los derechos tanto de los investigados como de terceras personas. Dichos problemas suelen originarse a partir de la anonimización de las direcciones IP, ya sea mediante programas informáticos o el uso de dispositivos públicos.

Cuando se trata de identificar a la persona asociada a una IP, independientemente de que se cuente con autorización judicial para ello o se utilicen medios propios de la policía que no requieran dicha autorización, surgen dudas sobre la posibilidad y exactitud de dicha identificación.

Uno de los principales inconvenientes radica en el uso de redes públicas para la comisión de actos delictivos. Se entiende por redes públicas aquellas que permiten el acceso a Internet a un gran número de personas, todas bajo la misma dirección IP proporcionada por el

proveedor de servicios[74]. En tales casos, la relación entre una dirección IP y un usuario concreto de esa red pública se complica, lo que podría llevar a la identificación errónea de una persona como presunta autora de un delito, afectando así derechos fundamentales, como el derecho a la presunción de inocencia del artículo 24.2 CE. Este problema también puede presentarse en el uso de redes privadas, donde una persona contrata una conexión a Internet, la cual puede ser utilizada posteriormente por otra para cometer un delito sin el conocimiento de quien la contrató y cuyo nombre aparece vinculado a la dirección IP.

De igual manera, este escenario puede darse en redes locales (*intranet*) utilizadas por empleados de empresas, universidades u organismos públicos[75]. En estos tres casos, es evidente la dificultad para identificar al usuario específico que, bajo esa dirección IP, pudo haber presuntamente cometido un acto delictivo, lo que puede vulnerar derechos como el de la tutela judicial efectiva.

Otro problema adicional proviene de la instalación de troyanos, el uso de proxis o técnicas de anonimización, como la navegación a través de la red TOR (The Onion Router). TOR o "el enrutador cebolla" en español, es un servicio que permite enmascarar las direcciones IP de sus usuarios, utilizando una red de repetidores administrados por voluntarios en todo el mundo[76]. Por

[74] LLOPIS NADAL, P., "Direcciones IP y presunto anonimato. Tras la identidad del usuario infractor de derechos de propiedad intelectual en Internet", *InDret Revista para el análisis del derecho,* nº 4 (2018), pág. 30.
[75] LLOPIS NADAL, P., Ibíd., págs 31 y 32.
[76] MACKEY, A., "Unreliable Informants: IP Addresses, Digital Tips and Police Raids How Police and Courts are Misusing

ello, cuando la policía identifica una dirección IP que ha utilizado este servicio, no es capaz de determinar quién es el autor del acto, lo que puede poner en riesgo las libertades y derechos de personas inocentes.

Este tipo de situaciones no se limitan únicamente a servicios como TOR; existen una gran cantidad de mecanismos que pueden ser utilizados para evitar la vinculación de una IP a una persona, como las Redes Privadas Virtuales (en inglés, Virtual Private Network, VPN), que permiten establecer una localización diferente a la real del usuario, o las IP "tipo NAT" (Network Address Translation), que permiten que varias redes se conecten a Internet bajo una misma dirección IP, actuando como una red intermedia que impide identificar a un usuario determinado[77].

Otro mecanismo similar utilizado para evitar la vinculación directa de una dirección IP con un usuario es el uso de proxis. Los proxis actúan como intermediarios entre el dispositivo de un usuario y la red de Internet, lo que permite ocultar la dirección IP real del usuario[78]. Cuando un usuario se conecta a Internet a través de un proxy, la dirección IP que se muestra a los servidores o sitios web es la del servidor proxy, no la del dispositivo del usuario. Este proceso de enmascaramiento dificulta

Unreliable IP Address Information and What They Can Do to Better Verify Electronic Tips", E*lectronic frontier foundation,* (2016), pág 11.

[77] CALVO LÓPEZ, D., Op. Cit., pág. 13.

[78] ARAVIND, T. N., MUKUNDH, A., VIJAYAKUMAR, R., "Tracing Ip Addresses Behind Vpn/Proxy Servers", *International Conference on Networking and Communications (ICNWC)*, (2023), pág. 1.

la identificación del usuario real y, por lo tanto, puede complicar la labor de las autoridades encargadas de investigar actos delictivos cometidos en línea.

Por lo tanto, es crucial que tanto la Policía Judicial como los tribunales comprendan las formas en que las personas se conectan a Internet y la posibilidad de que el usuario vinculado a una IP no sea el que haya realizado las acciones objeto de la investigación.

En conclusión, aunque las direcciones IP son herramientas esenciales en la investigación digital, su obtención y uso sin autorización judicial plantean serios desafíos en términos de protección de derechos fundamentales. La complejidad del consentimiento concedido a los proveedores de servicios, la incertidumbre en la protección de la privacidad y la posible injerencia sobre la intimidad de los datos de abonado, junto con la creciente utilización de técnicas de anonimización, dificulta la identificación precisa del usuario responsable. Esto puede derivar en vulneraciones del derecho a la intimidad, a la presunción de inocencia y a la tutela judicial efectiva. Por ello, es fundamental que se adopten medidas que aseguren la protección efectiva de la privacidad, sin comprometer la eficacia en la lucha contra el delito.

IV. AVANCES LEGISLATIVOS EUROPEOS Y SUS DESAFÍOS

La transformación digital ha revolucionado las dinámicas de investigación penal, introduciendo herramientas como el OSINT y el rastreo de direcciones IP que, si bien potencian la eficacia de las autoridades, plantean desafíos sin precedentes para los derechos fundamentales en el ámbito europeo. En este contexto,

la Unión Europea ha desarrollado un marco legislativo, encabezado por el Reglamento *E-Evidence* y el paquete normativo sobre privacidad digital, que busca armonizar la cooperación judicial e intenta responder a los retos actuales.

1. El REGLAMENTO *E-EVIDENCE.*

Ante el crecimiento de las investigaciones a través de la red, la UE aprobó el Reglamento 2023/1543 de 12 de julio, sobre las órdenes europeas de producción y de conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad a raíz de los procesos penales, también conocido como Reglamento *E-Evidence* que será aplicable a partir del 18 de agosto de 2026. Este reglamento prevé la creación de una Orden Europea de Producción, que permitirá que una autoridad judicial de un Estado miembro obtenga pruebas electrónicas directamente de un proveedor de servicios en otro Estado miembro, quien estará obligado a responder en un plazo de 10 días, y en un máximo de 8 horas en casos de emergencia, y de una Orden Europea de Conservación, por la que una autoridad judicial de un Estado miembro podría solicitar a un proveedor de servicios en otro Estado miembro que conserve datos específicos, en vista de una solicitud posterior de los mismos[79].

[79] COMISIÓN EUROPEA, "E-evidence - cross-border access to electronic evidence".
Disponible en:
https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en

Por lo que, en términos generales, el Reglamento establecería un mecanismo que permitiría a los jueces de un Estado miembro solicitar a los proveedores de servicios radicados en otra jurisdicción, aquellos datos electrónicos que fuesen necesarios para una investigación[80]. Su finalidad principal es fomentar la cooperación en materia de investigación a nivel internacional y agilizar los procedimientos para evitar perjudicar una investigación por la volatilidad de los datos alojados en la red[81].

Si bien su objetivo declarado es facilitar la lucha contra la delincuencia en la era digital, su aplicación en relación con técnicas de investigación digital como el OSINT y la obtención de direcciones IP plantea importantes consideraciones en cuanto a la vulneración de derechos fundamentales. En concreto, en el supuesto de unos datos de IP alojados en un servidor fuera del lugar en el que se realiza la investigación.

La orden para la solicitud de datos permite obtener y conservar pruebas electrónicas independientemente del lugar donde se encuentren los datos de los proveedores de servicios. Según el Reglamento, se considera proveedores de servicios a aquellas personas físicas o jurídicas que presten servicios como los de comunicaciones electrónicas, servicios de nombre de dominio de internet y de direcciones IP u otros servicios

[80] CUADRADO SALINAS, C., "La Directiva Europea y las Órdenes de Producción y Conservación de pruebas electrónicas en los procesos penales. ¿Nuevas perspectivas?", *IUS ET SCIENTIA,* vól. 9, nº 2 (2023), pág. 119.
[81] MURIEL DIÉGUEZ, J. A., "Los datos como prueba electrónica en el Reglamento E-Evidence", *Diario la Ley,* nº 94 (2025), pág. 2.

de la sociedad de la información[82], por lo que afecta directamente a la obtención de direcciones IP.

El Reglamento se fundamenta en el principio de confianza mutua entre Estados miembros, permitiendo que una autoridad judicial pida directamente a las plataformas digitales de otro Estado miembro del Reglamento. Así , por ejemplo, una fiscalía alemana podría solicitar datos a Telefónica España. En consecuencia, el representante de esa plataforma es quien recibe esa orden judicial y va a ser el encargado de escoger los datos a proporcionar, de este modo, se le da el poder de tratar con datos personales clave para una investigación a una empresa privada, lo que puede afectar la protección de los derechos de los ciudadanos[83].

En los Considerandos iniciales, este Reglamento pone de manifiesto la importancia de respetar los derechos fundamentales en el ámbito digital, especialmente el derecho a la vida privada y la protección de los datos personales, tal como establecen los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea[84]. Sin embargo, al dejar en manos de los Estados miembros la responsabilidad de aplicar las salvaguardias necesarias, se corre el riesgo de que existan desequilibrios en la protección de datos, especialmente cuando algunos Estados no cuenten con

[82] Véase artículo 3 Reglamento 2023/1543.
[83] VILÀ CUÑAT, A., "E-evidence: ¿una evidencia?", *Revista Sistema Penal Crítico*, vól. 4 (2023), pág. 4.
[84] Véase Considerando 13 Reglamento 2023/1543.

una regulación nacional adecuada a las nuevas técnicas de investigación digital.

En España, como se ha mencionado anteriormente, la LO 13/2015 intentó establecer un marco único para las diligencias de investigación tecnológicas, pero la falta de una ley específica para la investigación policial digital a través de OSINT o la obtención de direcciones IP puede generar inseguridad jurídica y menor protección de los derechos fundamentales en comparación con técnicas más reguladas como la interceptación de comunicaciones. Esta situación se agrava si otros Estados miembros tampoco cuentan con una normativa nacional adecuada para regular estas nuevas herramientas de investigación, ya que ello deja la aplicación de las salvaguardias de los derechos en manos de la interpretación y discrecionalidad de las autoridades nacionales[85], lo que puede derivar en desigualdades significativas en cuanto a la protección de la privacidad y los datos personales. Aunque el considerando 10 del Reglamento reconoce la importancia del respeto a los derechos fundamentales, la forma en que este respeto se materializa en la práctica puede variar entre Estados.

[85] En el Considerando 15 del Reglamento 2023/1543 se subraya la responsabilidad de las autoridades de los Estados miembros de asegurar una adecuada protección de los datos personales: *"En particular, los Estados miembros deben garantizar que se apliquen las políticas y medidas adecuadas en materia de protección de datos a la transmisión de datos personales por parte de las autoridades pertinentes a los prestadores de servicios para los fines del presente Reglamento, incluidas medidas destinadas a garantizar la seguridad de los datos".*

Por otro lado, el Reglamento *E-Evidence* establece la relevancia de las direcciones IP en el marco de las investigaciones policiales y subraya que estos datos deben estar plenamente protegidos, ya que pueden ser utilizados como prueba electrónica. Sin embargo, dentro de la información extraída de las direcciones IP, distingue entre los datos de tráfico y los datos de abonado[86]. Para obtener los primeros, se requiere el cumplimiento de requisitos más rigurosos: su solicitud debe estar supervisada por una autoridad judicial y vinculada a la investigación de infracciones penales de especial gravedad. En cambio, para obtener los datos de abonado basta con que la orden sea emitida o validada por un fiscal competente. Este aspecto ha sido señalado por el Comité Económico Social Europeo en un Dictamen[87] en el que mencionaba que los datos de abonado deben considerarse como datos de carácter personal, por lo que la orden debería ser acordada y emitida por una autoridad judicial, en lugar de por un fiscal[88]. Asimismo, el Consejo de la Abogacía Europea ha señalado el problema de esta distinción, establece que la falta de

[86] Véase Considerando 36 Reglamento 2023/1543.
[87] Dictamen del Comité Económico y Social Europeo sobre la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal [COM(2018) 225 final — 2018/0108 (COD)] — Propuesta de Directiva del Parlamento Europeo y del Consejo por la que se establecen normas armonizadas para la designación de representantes legales a efectos de recabar pruebas para procesos penales [COM(2018) 226 final — 2018/0107(COD)].
[88] Conclusión 1.7. del Dictamen del Comité Económico y Social Europeo.

concreción sobre lo que se considera dato de abonado y dato de acceso puede generar situaciones de inseguridad jurídica y considera fundamental ampliar las garantías a los datos de abonado[89].

Esta diferenciación, que también se refleja en el ordenamiento jurídico español, se basa en la consideración de que los datos de abonado presentan un menor nivel de sensibilidad y, por ende, una menor afectación a los derechos fundamentales. No obstante, como se ha señalado previamente, los datos de abonado pueden contener información detallada sobre los servicios utilizados por el usuario e incluso su identidad, lo que permite la elaboración de perfiles altamente precisos sobre los investigados y, por tanto, llegar a suponer una injerencia en los derechos igual de grave que el conocimiento de otros datos como los de tráfico. Por lo que, si algunos Estados miembros consideran la obtención de ciertos datos como direcciones IP requieren de menores requisitos que otros, podría llevar a situaciones en las que los datos de un ciudadano de un Estado con mayor protección se obtengan con estándares inferiores por una autoridad de otro Estado con menor regulación.

[89] CONSEJO DE LA ABOGACÍA EUROPEA, "Posición de CCBE sobre la propuesta de Reglamento de la Comisión sobre las Órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal", pág. 5 (2018). Disponible en: https://www.abogacia.es/wp-content/uploads/2019/03/Posicionamiento-sobre-ordenes-europeas-de-entrega-y-conservacion-de-pruebas-electronicas-a-efectos-de-enjuiciamiento-penal.pdf

Sumado a esto, el European Law Institute recogió una serie de recomendaciones[90] sobre la necesidad de incluir salvaguardias dirigidas a evitar manipulaciones y problemas de autenticidad de las pruebas electrónicas[91]. Esto se correlaciona con el problema ya presentado anteriormente de la fragilidad de la autenticidad de la información obtenida a través de fuentes como OSINT. La investigación mediante OSINT no tiene un mecanismo de control similar al de la interceptación de comunicaciones telefónicas y telemáticas que asegure la veracidad de los datos, lo que hace que esta información pueda ser fácilmente modificada. De sobremanera, una de las principales exigencias en la presentación de pruebas en el proceso penal es que se haya respetado la cadena de custodia, lo que asegura que la prueba no haya sufrido modificaciones, esta necesidad se acentúa en el caso de las pruebas electrónicas, debido a su forma de almacenamiento. El Reglamento *E-Evidence*, tal como está redactado, no incluye mecanismos específicos para garantizar la integridad de los datos usados como prueba electrónica, lo que resalta la necesidad de regulaciones

[90] EUROPEAN LAW INSTITUTE. Propuesta de Regulación de la Admisibilidad Mutua de Prueba y Prueba electrónica en los procesos penales dentro de la Unión Europea. Publicada el 8 de Mayo de 2023. Disponible en: https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Proposal_for_a_Directive_on_Mutual_Admissibility_of_Evidence_and_Electronic_Evidence_in_Criminal_Proceedings_in_the_EU.pdf

[91] En la Propuesta del European Law Institute, se señala que, en el contexto de las pruebas electrónicas transfronterizas, se reconocen generalmente dos grandes desafíos, siendo uno de ellos cómo la naturaleza intangible de los datos electrónicos los hace susceptibles a ser manipulados con facilidad.

y salvaguardias más específicas para este tipo de investigación digital a nivel europeo.

El Informe SIRIUS 2024 sobre la prueba electrónica transfronteriza en la Unión Europea ofrece una visión actualizada sobre los retos que enfrenta la aplicación del Reglamento *E-Evidence* una vez entre en vigor. El Proyecto SIRIUS, creado en 2017 por la Europol, se trata de una herramienta que permite facilitar la gestión de la información digital a través de directrices estandarizadas, herramientas de investigación, repositorios de datos de los proveedores de servicios y una plataforma de comunicación para los investigadores[92]. Esta base de conocimiento permite a los investigadores identificar rápidamente qué entidades podrían poseer la información relevante para una investigación.

Este informe de 2024 destaca los desafíos a los que se enfrentan los investigadores a la hora de obtener datos necesarios[93]. Revela, entre otros aspectos, que el volumen creciente de solicitudes, que se prevé que aumente con la entrada en vigor del Reglamento *E-Evidence*, y la rápida evolución legislativa, representan desafíos significativos para los proveedores de servicios. Se especifica que la fragmentación existente entre los

[92] Información sobre el Proyecto SIRIUS disponible en: https://www.europol.europa.eu/media-press/newsroom/news/europol-launches-sirius-platform-to-facilitate-online-investigations

[93] EUROPOL y EUROJUST, "SIRIUS EU Electronic Evidence Situation Report 2024*", 6th ANNUAL SIRIUS EU ELECTRONIC EVIDENCE SITUATION REPORT,* pág. 60. Disponible en: https://www.europol.europa.eu/cms/sites/default/files/documents/SIRIUS_E_Evidence_Situation_Report_2024.pdf

Estados miembros provoca que los proveedores reciban solicitudes de distintos funcionarios y tengan que contactar con cada uno para especificar los requisitos. De este modo, se comprueba cómo el problema que conlleva la confianza mutua y el dejar la gestión a las plataformas de servicio, anteriormente destacado respecto al Reglamento *E-Evidence*, se halla cada vez más presente por el incremento de solicitudes y las complicaciones que tienen las plataformas para proceder con la entrega o la conservación de datos.

Asimismo, el informe menciona cómo la divergencia regulatoria entre países puede generar problemas. Los proveedores de servicios, especialmente aquellos que operan en varios países, deben estar al tanto de las legislaciones nacionales y la falta de unidad normativa hace que el esfuerzo requerido en estas circunstancias constituya un desafío para los proveedores.

Por último, destaca un problema novedoso, pero relacionado con los problemas de la facilidad de manipular los datos en la red. El aumento del volumen de solicitudes complica la labor de detección de solicitudes fraudulentas, los proveedores pueden no ser capaces de comprobar la identidad de la autoridad solicitante y esto puede afectar a la privacidad de los involucrados. Anteriormente se había destacado la inseguridad que pueden generar los datos en internet al ser fácilmente alterados, por lo que una investigación que se fundamentase en dichos datos modificados podía conllevar a conclusiones erróneas y una condena incorrecta.

Ahora, además, se presenta un nuevo desafío: la posibilidad de solicitar datos directamente a proveedores

de servicios a través de esta nueva regulación europea, basándose en la confianza mutua, sin un control exhaustivo, puede conllevar a situaciones en las que sujetos no autorizados lleven a cabo solicitudes fraudulentas a los proveedores y estos sean incapaces de autentificar su identidad. De este modo, se estaría dando acceso a datos muy personales, incluidos los datos de abonado, que, como ya se ha expuesto, contienen información sobre la identidad y comportamientos del usuario a personas cuyas intenciones pueden no ser legítimas. Esta obtención de datos por parte de personal no autorizado supondría una gran injerencia en los derechos fundamentales, concretamente en el de la intimidad personal y familiar y el secreto de las comunicaciones.

Finalmente, el informe concluye con una serie de recomendaciones orientadas a la futura implementación del Reglamento *E-Evidence*, destacando la necesidad de que los principales actores implicados, autoridades judiciales, cuerpos de investigación y proveedores de servicios, se preparen adecuadamente para su aplicación. Asimismo, se subraya la importancia de reforzar la cooperación y la confianza mutua entre ellos, aprovechando herramientas como la plataforma SIRIUS para facilitar una implementación coordinada del nuevo marco normativo en materia de prueba electrónica.

En definitiva, la entrada en vigor del Reglamento *E-Evidence* supondrá un avance significativo en la cooperación judicial europea para la obtención de pruebas electrónicas transfronterizas, facilitando el acceso a datos clave como las direcciones IP, incluso cuando estos se encuentren alojados fuera de las fronteras nacionales. Sin embargo, este nuevo marco

plantea importantes desafíos en materia de protección de derechos fundamentales, especialmente por la falta de armonización normativa entre los Estados miembros y la delegación de funciones sensibles en manos de proveedores privados, lo que puede generar inseguridad jurídica y riesgos para la privacidad y la integridad de los datos.

Solo mediante el refuerzo de las salvaguardias, la cooperación estrecha y mecanismos de autenticación y control, tal y como indica el informe SIRIUS 2024, se podrán evitar tanto manipulaciones como solicitudes fraudulentas, y garantizar que la eficacia en la lucha contra la delincuencia digital no suponga un retroceso en las libertades y derechos fundamentales de los ciudadanos europeos.

2. PRIVACIDAD EN LA ERA DIGITAL: ÚLTIMAS NORMAS DE LA UE.

En 2020, la Comisión Europea emitió una comunicación sobre una Estrategia Europea de Datos[94], en la que recalcaba la importancia de los datos en una realidad marcada por la transformación digital. Asimismo, se mencionaba el papel de la UE como referente a nivel mundial y la responsabilidad que tiene en relación con el correcto uso de los datos. Estos datos, como se ha ido mostrando a lo largo del trabajo, presentan desafíos

[94] Véase COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES: Una Estrategia Europea de Datos en Bruselas, 19.2.2020 COM(2020) 66 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0066

para los derechos fundamentales, especialmente en el contexto de investigaciones basadas en OSINT o la obtención de direcciones IP. Esta comunicación toma como base el Reglamento General de Protección de Datos (RGPD)[95], por el cual se creaba el marco general respecto a la regulación de la protección de datos personales. No obstante, este reglamento presenta limitaciones significativas, por ejemplo, su ámbito de aplicación restringido, por el cual solo se protegen datos personales[96], excluyendo información anonimizada o pseudonimizada. Esta información anonimizada, puede reidentificarse mediante técnicas avanzadas como las técnicas OSINT, identificando al sujeto, en este caso, una persona investigada, y, por tanto, vulnerando su privacidad. Además, la información como las direcciones IP quedan fuera del alcance de esta normativa, facilitando su uso sin garantías suficientes. Ante estas carencias, la UE ha ido impulsando un paquete legislativo complementario para adaptarse a los nuevos retos digitales, con leyes como la Ley de Mercados Digitales (DMA), Ley de Servicios Digitales (DSA), Ley de Gobernanza de Datos (DGA), Ley de Inteligencia Artificial (AI Act) o la reciente Ley de Datos (DA).

La Ley de Mercados Digitales regula a los "guardianes de acceso", esto es, las grandes plataformas como Google, para evitar prácticas anticompetitivas, pero también

[95] 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.

[96] LÓPEZ-LAPUENTE, L., "La nueva regulación europea de los datos: cómo dar forma al futuro digital de Europa", *Actualidad Jurídica Uría Menéndez,* nº 61 (2023), pág. 52.

incluye obligaciones de transparencia en el uso de datos que podría mejorar la calidad de la información que recibe la población y, por tanto, hacer que el consentimiento sea más informado y se reduzca así uno de los problemas identificados. La Ley de Servicios Digitales exige mayor responsabilidad a las plataformas en la moderación de contenidos, lo que podría limitar el acceso indiscriminado a datos públicos para el empleo de técnicas OSINT.

Por su parte, la Ley de Gobernanza de Datos busca facilitar el intercambio de datos entre los países de la UE de forma segura, sin embargo, sigue conllevando riesgos cuando se trata de datos que, aunque no sean clasificados como "personales" bajo el RGPD, pueden derivar en vulneraciones indirectas de derechos fundamentales. La Ley de Inteligencia Artificial pretende evitar los sesgos en los sistemas de IA al evaluar los perfiles de los investigados en un delito penal[97], paso fundamental para evitar calificaciones erróneas si se usa la Inteligencia Artificial en las técnicas OSINT.

Sin embargo, al dejar la responsabilidad sobre el cumplimiento de esta ley a los proveedores de sistemas de IA, puede correr el riesgo de que estos no cumplan con las exigencias básicas. Por último, la Ley de Datos, aplicable a partir de septiembre de 2025, regula el acceso y uso de datos generados por dispositivos IoT (Internet de las Cosas), es decir, aquellos objetos que se

[97] EUROPEAN ARTIFICIAL INTELLIGENCE ACT, "High-level summary of the Artificial Intelligence Act", *Future of Life Institute*, (2024).

conectan a internet y recopilan información[98]. Estos dispositivos pueden generar datos como direcciones IP que pueden revelar una gran cantidad de información personal, como se ha destacado con anterioridad, por lo que la Ley de Datos pretende garantizar que los usuarios tengan el control sobre esta información, incluso cuando no se clasifique como "personal" según el RGPD, suponiendo así un avance importante en la protección de los usuarios de Internet.

En definitiva, el marco normativo europeo en materia de protección de datos está experimentando una evolución significativa para adaptarse a los retos de la era digital. Si bien el RGPD sentó las bases para la protección de datos personales, sus limitaciones, especialmente en lo relativo a datos anonimizados, han quedado en evidencia ante el avance de técnicas como el OSINT.

Por otro lado, el paquete legislativo complementario representa un esfuerzo por cerrar estas brechas, estableciendo mayores garantías en el uso de datos y reforzando los derechos individuales. Sin embargo, como hemos analizado, persisten riesgos significativos, particularmente en lo que respecta al uso de información técnicamente no personal que puede vulnerar derechos fundamentales. La efectividad de este nuevo marco dependerá en gran medida de su aplicación rigurosa, de la supervisión independiente y de la capacidad para adaptarse a los rápidos avances tecnológicos.

[98] Más información sobre esta ley disponible en la web oficial de la UE: Una estrategia Europea de datos: Ley de Datos. Disponible en: https://digital-strategy.ec.europa.eu/es/policies/data-act

V. CONCLUSIONES.

La transformación digital ha supuesto un cambio radical en las formas de investigar delitos, dando lugar a un auge de las técnicas de investigación tecnológica y permitiendo a las autoridades policiales acceder a grandes cantidades de información a través de medios cada vez más sofisticados. En este contexto, dos herramientas destacan por su relevancia y, al mismo tiempo, por el vacío legal que las rodea: la Inteligencia de Fuentes Abiertas (OSINT) y la obtención de direcciones IP.

PRIMERA: Uno de los principales contrastes que revela este trabajo es la diferencia normativa existente entre las diligencias de investigación. Mientras que la interceptación de las comunicaciones telefónicas y telemáticas se encuentra altamente regulada y sujeta a estrictas garantías judiciales, el uso de técnicas como OSINT o la obtención de direcciones IP carecen de una regulación específica. Como se ha analizado, la interceptación de las comunicaciones requiere de una autorización judicial previa y está sujeta al principio de proporcionalidad, sin embargo, el uso del OSINT al basarse en la recopilación de información accesible públicamente no requiere control judicial y se corre el riesgo de no discernir correctamente la información relevante para la investigación de la que no lo es, incumpliéndose así el principio de proporcionalidad. Esto genera una reducción significativa de las garantías legales, pese a que los efectos sobre la privacidad pueden ser similares o incluso mayores, dada la capacidad del OSINT de reconstruir perfiles completos e íntimos a partir de datos dispersos. Esto ocurre de igual manera respecto al secreto de las comunicaciones,

ampliamente protegido para la interceptación de las comunicaciones, mientras que se enfrenta a desafíos derivados del empleo del OSINT cuando se accede a conversaciones en espacios cerrados en Internet.

SEGUNDA: Las técnicas OSINT presentan otros desafíos relacionados con el consentimiento, la sensación de privacidad de los individuos, el tratamiento de los datos o la fiabilidad de los datos obtenidos, así como el dilema entre lo que se considera información pública y privada. Igualmente, se plantea el problema de la introducción de la IA a las técnicas OSINT, que puede afectar al principio de igualdad y no discriminación y al derecho a un juicio con todas las garantías si esta Inteligencia está sesgada, cuestión que como se ha visto, preocupa a la UE y se pretende paliar con la Ley de Inteligencia Artificial.

TERCERA: En el caso de las direcciones IP, la legislación permite su obtención sin autorización judicial cuando se utilizan medios propios de la Policía o cuando se solicitan únicamente los datos de abonado. No obstante, esta distinción normativa no siempre se traduce en una menor afectación al derecho a la intimidad, ya que el análisis conjunto de estos datos puede permitir la identificación detallada de una persona, sin que medie su consentimiento informado. Además, la identificación de una persona a través de una dirección IP no es fiable en muchos casos, debido al uso de redes públicas, dispositivos compartidos o herramientas de anonimización, lo que puede llevar a errores de atribución delictiva y comprometer el derecho a la presunción de inocencia.

CUARTA: El contraste entre la normativa de interceptaciones y el OSINT y las direcciones IP refleja

una asimetría en la protección de los derechos fundamentales. En primer lugar, respecto al derecho a la privacidad y a la intimidad personal y familiar: la recopilación de datos personales, aunque públicos, sin el consentimiento del individuo, puede invadir su privacidad. En segundo lugar, en relación con el derecho al secreto de las comunicaciones, el uso de OSINT puede implicar la revelación de conversaciones privadas. Y, por último, se ven afectados otros derechos como el de la presunción de inocencia al no garantizarse mecanismos neutrales de clasificación de la información o de identificación correcta del usuario investigado.

QUINTA: A nivel europeo, esta situación se agrava. Aunque la Unión Europea ha impulsado normas como la Orden Europea de Producción, la Orden Europea de Conservación y diversos reglamentos sobre protección de datos y servicios digitales, el marco legal de la UE aún no contempla de forma específica el uso de estas diligencias de investigación tecnológicas. El reciente Reglamento *E-Evidence* supone un paso importante hacia la armonización de estas prácticas en el entorno digital. Aunque no regula de forma directa las técnicas de investigación digital como el OSINT, sí afecta de manera significativa a la obtención de direcciones IP al permitir a las autoridades judiciales solicitar estos datos directamente a los proveedores de servicios, sin intervención de la autoridad del Estado donde estos están establecidos. Sin embargo, el hecho de dejar en manos de estos proveedores la selección y entrega de los datos, así como las diferencias nacionales en cuanto a garantías jurídicas, puede generar desigualdades en la protección de derechos fundamentales entre los distintos Estados miembros. Además, el Reglamento no

establece mecanismos claros que aseguren la autenticidad y la cadena de custodia de los datos, una omisión crítica en el caso de pruebas digitales especialmente vulnerables a manipulaciones. Tampoco la jurisprudencia del Tribunal Europeo de Derechos Humanos ha abordado con claridad su uso. Actualmente, son tratadas como una técnica más de investigación, sin embargo, la inseguridad jurídica generada por esta falta de regulación específica representa un riesgo, ya que permite un uso por parte de la Policía Judicial sin un pleno respeto a la intimidad personal y familiar y al secreto de las comunicaciones.

SEXTA: Por lo tanto, esta laguna legal debería ser subsanada mediante una regulación que establezca límites claros, requisitos de motivación, procedimientos de autorización y mecanismos de control para estas nuevas técnicas de investigación. Solo así se garantizará un equilibrio adecuado entre la eficacia de la acción penal y la salvaguarda de los derechos fundamentales en la era digital. Además, resultaría necesario complementar esta regulación con un modelo reforzado de consentimiento informado digital, que contribuya a reducir la asimetría informativa existente entre usuarios y operadores digitales. Este modelo debería obligar a las plataformas a informar de manera accesible, clara y comprensible sobre qué datos se recogen, incluyendo direcciones IP, con qué fines y si pueden ser usados en investigaciones penales. Solo mediante una combinación de un control judicial efectivo y un consentimiento realmente informado se podrá consolidar un entorno digital respetuoso con los derechos fundamentales y adaptado a los desafíos del siglo XXI.

VI. BIBLIOGRAFÍA:

ALFONSO RODRÍGUEZ, A. J., "Interceptación de comunicaciones telefónicas, seguridad(es) y garantías procesales", *Ciencia Policial,* nº *182*, págs. 97–144. https://doi.org/10.14201/cp.31812

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Informe 327/2003", (2003). Disponible en: https://www.aepd.es/documento/2003-0327.pdf

ÁLVAREZ MEDIALDEA, A.F., "Cuestiones controvertidas en torno a la diligencia de captación y grabación de las comunicaciones orales mediante la utilización de dispositivos electrónicos. Determinación del concepto de encuentro", *Revista Penal,* nº 51 (2023), págs. 9-32.

ARAVIND, T. N., MUKUNDH, A., VIJAYAKUMAR, R., "Tracing Ip Addresses Behind Vpn/Proxy Servers", *International Conference on Networking and Communications (ICNWC)*, (2023), págs. 1-10. Disponible en: DOI: 10.1109/ICNWC57852.2023.10127335.

ASENCIO MELLADO, J.M. y FUENTES SORIANO, O., *Derecho procesal penal,* Tirant lo Blanch, Valencia, 1.ª edición, 2019.

BARONA VILAR, S., "El algoritmo en la prueba y en la decisión judicial: ¿instrumental o funcional?", BUSTAMANTE RÚA, M. M., HENAO OCHOA, A. DEL P., RAMÍREZ CARVAJAL, D. M. (Coords.), *La justicia en la era de la revolución tecnológica,* Institución Universitaria de Envigado, Envigado, 2023, págs. 9-34.

BARONA VILAR, S., "Justicia con algoritmos e inteligencia artificial, ¿acuerpando garantías y derechos procesales o liquidándolos?", *Derechos y Libertades,* nº 51, Época II (2024), págs. 83-115. DOI: https://doi.org/10.20318/dyl.2024.8584

BARRIO ANDRÉS, M., *Derecho Público e Internet: la actividad administrativa de regulación de la Red*, Instituto Nacional de Administración Pública (INAP), Madrid, 2017, 1ª edición.

BASHIR, M., HAYES, C., LAMBERT, A. D., KESAN, J. P., "Online privacy and informed consent: The dilemma of information asymmetry" *Proceedings of the Association for Information Science and Technology*, vol. 52, nº 1 (2015), págs 1-10. Disponible en: DOI10.1002/pra2.2015.145052010043.

BERTONI, E., "Las prácticas OSINT, ¿son amigas o enemigas de los derechos humanos?", *CELE Research,* nº 58 (2023), págs. 2-31. Disponible en: DOI: http://dx.doi.org/10.2139/ssrn.5157884

BUENO DE MATA, F., BUJOSA VADELL, L. (pr.), *Las diligencias de investigación penal en la cuarta revolución industrial. Principios teóricos y problemas prácticos,* Thomson Reuters Aranzadi, Navarra, 2019, 1.ª edición.

BUENO DE MATA, F., "Técnicas de ciberinteligencia aplicables a la investigación de delitos de odio en redes abiertas: reflexiones críticas", en AGUILAR CÁRCELES, M. M., SOTO CASTRO, J. E., VINAGRE GONZÁLEZ, A. M., (Dirs.), *Delitos de odio. Un abordaje multidisciplinar*, J.B. Bosch, Barcelona, 2023, págs. 47-67.

BUENO DE MATA, F., *Investigación y prueba de delitos de odio en redes sociales técnicas OSINT e inteligencia policial,* Tirant lo Blanch, Valencia, 2023, 1ª Edición.

CABEZUDO RODRÍGUEZ, N., "Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal", *Boletín del Ministerio de Justicia*, vol. 70, nº 2186, (2016), págs. 7-60. Disponible en: http://tinyurl.com/4tkv5whf.

CALVO LÓPEZ, D., "Capacidades de actuación del ministerio fiscal y la policía judicial tras la reforma procesal operada por la ley orgánica 13/2015: en especial la obtención de direcciones IP y numeraciones IMEI e IMSI (los apartados k) a m) del art. 588 ter de la LECRIM)", *Jornadas de Especialistas celebradas en el Centro de Estudios Jurídicos de Madrid*, 16 y 17 febrero de 2017, págs. 1-29. Disponible en: https://www.fiscal.es/documents/20142/99680/Ponencia+Calvo+L%C3%B3pez%2C+David+%282017%29.pdf/257930af-0b51-6bfb-4640-1205a04d1a74?t=1531136313090

CASANOVA MARTÍ, R. y CERRATO GURI, E., "La emisión de una orden europea de investigación para la obtención de prueba transfronteriza y su introducción en el proceso penal español", *Revista de Derecho Comunitario Europeo*, nº 62 (2019), págs 197-232. Disponible en: DOI https://doi.org/10.18042/cepc/rdce.62.06

COLOMER HERNÁNDEZ, I., "Limitaciones en el uso de la información y los datos personales en un proceso penal digital", FREITAS, P. M., (Coord.), *El proceso penal ante*

una nueva realidad tecnológica europea, Thomson Reuters Aranzadi, Navarra, 2023, págs. 39-74.

COMISIÓN EUROPEA, "E-evidence - cross-border access to electronic evidence". Disponible en: https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES: Una Estrategia Europea de Datos en Bruselas, 19.2.2020 COM (2020) 66 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0066

CONSEJO DE LA ABOGACÍA EUROPEA, "Posición de CCBE sobre la propuesta de Reglamento de la Comisión sobre las Órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal", págs. 1-12 (2018). Disponible en: https://www.abogacia.es/wp-content/uploads/2019/03/Posicionamiento-sobre-ordenes-europeas-de-entrega-y-conservacion-de-pruebas-electronicas-a-efectos-de-enjuiciamiento-penal.pdf

CUADRADO SALINAS, C., "La Directiva Europea y las Órdenes de Producción y Conservación de pruebas electrónicas en los procesos penales. ¿Nuevas perspectivas?", IUS ET SCIENTIA, vól. 9, nº 2 (2023), págs 117-135.

DAMJAN, M., "The protection of privacy of the IP address in Slovenia", *Law, Identity and Values,* vol. 2 (2023),

págs 25-43. Disponible en: DOI: https://doi.org/10.55073/2022.2.25-43

Dictamen del Comité Económico y Social Europeo sobre la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal [COM(2018) 225 final — 2018/0108 (COD)] — Propuesta de Directiva del Parlamento Europeo y del Consejo por la que se establecen normas armonizadas para la designación de representantes legales a efectos de recabar pruebas para procesos penales [COM(2018) 226 final — 2018/0107(COD)].

EIJKMAN, Q., WEGGEMANS, D., "Open source intelligence and privacy dilemmas Is it time to reassess state accountability?", *Security and Human Rights*, vol. 23 (2013), págs 2-11. Disponible en DOI: 10.1163/18750230-99900033.

EUROPEAN ARTIFICIAL INTELLIGENCE ACT, "High-level summary of the Artificial Intelligence Act", Future of Life Institute, (2024), Disponible en: https://artificialintelligenceact.eu/high-level-summary/ [fecha de consulta: 02/05/2025].

EUROPEAN LAW INSTITUTE. Propuesta de Regulación de la Admisibilidad Mutua de Prueba y Prueba electrónica en los procesos penales dentro de la Unión Europea. Publicada el 8 de mayo de 2023. Disponible en: https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Proposal_for_a_Directive_on_Mutual_Admissibility_of_Evidence_and_Electronic_Evidence_in_Criminal_Proceedings_in_the_EU.pdf

EUROPOL y EUROJUST, "SIRIUS EU Electronic Evidence Situation Report 2024*", 6th ANNUAL SIRIUS EU ELECTRONIC EVIDENCE SITUATION REPORT,* págs 1-73. Disponible en: https://www.europol.europa.eu/cms/sites/default/files/documents/SIRIUS_E_Evidence_Situation_Report_2024.pdf

FERRANTE, E., "Inteligencia artificial y sesgos algorítmicos. ¿Por qué deberían importarnos?", *Nueva Sociedad,* nº 294 (2021), págs. 27-37. Disponible en: https://nuso.org/articulo/inteligencia-artificial-y-sesgos-algoritmicos/.

FRIEDMAN B., FELTEN E., y HOWE, D.C, "Informed Consent in the Mozilla Browser: Implementing Value-Sensitive Design", *Proceedings of the 35th Hawaii International Conference on System Sciences,* vol. 8 (2002), págs. 1-10. Disponible en: DOI: 10.1109/HICSS.2002.994366.

GARRIDO CARRILLO, F. J., "Insuficiencias y limitaciones de la Orden Europea de Investigación (OEI)", Revista de Estudios Europeos, Nº extraordinario monográfico 1 (2019), págs 206-224.

GIMENO SENDRA, J., "La intervención de las comunicaciones telefónicas y electrónicas", *El notario del siglo XXI.* Revista del Colegio Notarial de Madrid, nº. 39, (2011), págs. 1-0. Disponible en: https://legado.elnotario.es/hemeroteca/revista-39/697-la-intervencion-de-las-comunicaciones-telefonicas-y-electronicas-0-2863723191305737

HULSEN, L TEN., "Open Sourcing Evidence from the Internet- the Protection of Privacy in Civilian Criminal

Investigations Using Osint (Open-Source Intelligence)", *Amsterdam Law Forum*, vol. 12, nº 2 (2020), págs. 1-45. [Fecha de consulta: 11-03-2025] Disponible en: https://research.ebsco.com/linkprocessor/plink?id=d233c6ed-3fd0-3893-9354-da44d304da70

LANDE, D., SHNURKO-TABAKOVA, E., "OSINT as a part of cyber defense system", *Theoretical and Applied Cybersecurity*, vol. 1, nº 1 (2019), págs. 103-108. Disponible en: DOI: 10.20535/tacs.2664-29132019.1.169091

LENOIR-GRAND PONS, R., "Análisis de riesgo, prevención y comunicación en la gestión de crisis", MOLINER GONZÁLEZ, J. A., GONZÁLEZ-RABANAL, M. C. (Dirs.), *Seguridad, control de fronteras y derechos humanos. Gestión pública de las crisis sociales,* Dykinson, Madrid, 2022, págs. 237-256. Disponible en: DOI: 10.2307/jj.1866699.13

LLOPIS NADAL, P., "Direcciones IP y presunto anonimato. Tras la identidad del usuario infractor de derechos de propiedad intelectual en Internet", *InDret Revista para el análisis del derecho,* nº 4 (2018), págs. 1-41.

LÓPEZ FERIA, A., "Nuevas tecnologías e interceptación de las comunicaciones telefónicas y telemáticas", *Revista Española de Derecho Militar,* nº 111 y 112 (2019), págs. 213-245.

LÓPEZ JIMÉNEZ, R., *Victimización sexual y nuevas tecnologías: desafíos probatorios,* Dykinson, Madrid, 2021, 1ª edición.

LÓPEZ-LAPUENTE, L., "La nueva regulación europea de los datos: cómo dar forma al futuro digital de Europa", *Actualidad Jurídica Uría Menéndez,* nº 61 (2023), págs. 50-71.

MACKEY, A., "Unreliable Informants: IP Addresses, Digital Tips and Police Raids How Police and Courts are Misusing Unreliable IP Address Information and What They Can Do to Better Verify Electronic Tips", E*lectronic frontier foundation,* (2016), págs. 1-22.

MARTÍNEZ GALINDO, G., "Problemática jurídica de la prueba digital y sus implicaciones en los principios penales", *Revista Electrónica de Ciencia Penal y Criminología,* nº 24-23 (2022), págs. 1-38. Disponible en: http://criminet.ugr.es/recpc/24/recpc24-23.pdf

MATTEO PASQUINELLI, V. J., "El Nooscopio de manifiesto. La inteligencia artificial como instrumento de extractivismo del conocimiento.", *La Fuga,* nº 25 (2021), págs. 1-20. [Fecha de consulta: 07-03-2025] Disponible en: http://2016.lafuga.cl/el-nooscopio-de-manifiesto/1053

MILLETT, E., "Open-Source Intelligence, Armed Conflict, and the Rights to Privacy and Data Protection", *Security and Human Rights Monitor,* (2023), págs. 1-19. Disponible en: DOI: 10.58866/HQKE7327

MONTE, M., SÁNCHEZ. S.I., "Tensiones constitucionales entre el derecho a la intimidad y el ciberpatrullaje en la investigación criminal. Análisis del Protocolo General para la Prevención Policial del Delito con Uso de Fuentes Digitales Abiertas", Revista Pensamiento Penal, (2021), págs. 1-15. Disponible en:

https://www.pensamientopenal.com.ar/system/files/2021/04/doctrina89035.pdf

MURIEL DIÉGUEZ, J. A., "Los datos como prueba electrónica en el Reglamento E-Evidence" en *Diario la Ley,* nº 94 (2025), págs. 1-10.

ORTIZ PRADILLO, J. C., "La investigación del delito en la era digital. Los derechos fundamentales frente a las nuevas medidas tecnológicas de investigación", *Estudios de Progreso, Fundación Alternativas,* nº 72 (2013), págs 1-59.

ORTIZ PRADILLO, J. C., "Dispositivos o medios técnicos de seguimiento y localización en el proceso penal", RODRÍGUEZ LAINZ, J. L. (Dir.), *Diligencias de investigación tecnológica,* Cuadernos digitales de formación nº 5, Consejo General del Poder Judicial, Madrid, 2018, págs. 40-77. Disponible en: DOI: https://doi.org/10.62659/CF1800502

PALOP BELLOCH, M., "Las medidas de investigación tecnológica", *Justicia: Revista de derecho procesal,* nº 2 (2017), págs. 443-490, pág.

PASTOR-GALINDO, J., NESPOLI, P., MÁRMOL, F. G., & PÉREZ, G. M, "The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends", *IEEE access,* vol. 8 (2020), págs. 10282-10304.

PERALTA GUTIÉRREZ, A., AGUIRRE ALLENDE, P., "El TJUE y el acceso a los datos de abonado en el seno de la instrucción penal", *Diario la Ley,* nº 9420 (2019), págs. 1-11.

PÉREZ GIL, J., "Medidas de investigación tecnológica en el proceso penal español: privacidad vs. eficacia en la persecución", en: BRIGHI, R., PALMIRANI, M. y SÁNCHEZ JORDÁN, M.E (dirs.), *Informatica giuridica e informatica forense al servizio della società della conoscenza. Scritti in onore di Cesare Maioli*, Editorial Aracne, Roma, 2018.

RAYÓN BALLESTEROS, M. C., "Medidas de investigación tecnológica en el proceso penal la nueva redacción de la Ley de Enjuiciamiento Criminal operada por la Ley Orgánica 13/2015", *Anuario jurídico y económico escurialense,* nº 52 (2019), págs. 179-204.

RICHARD GONZÁLEZ, M., "Conductas susceptibles de ser intervenidas por medidas de investigación electrónica. Presupuestos para su autorización"**,** *Diario La Ley*, nº 8808 (2016), págs. 1-16.

ROJO TORRES J. D., "OsiNET desarrollo de una herramienta de integración OSINT", *Alcalibe: Revista Centro Asociado a la UNED Ciudad de la Cerámica,* nº 23 (2023), págs. 179-215.

TORO-ALVAREZ M. M., BONILLA-DUITAMA M.L., PARADA JAIMES W.D., "Investigación del Cibercrimen y de los Delitos Informáticos Utilizando Inteligencia de Fuentes Abiertas de Información (OSINT)", *Researchgate*, (2018), págs. 1-11. DOI: 10.13140/RG.2.2.21594.59849.

VARONA JIMÉNEZ, A., "Aspectos relevantes de la interceptación de las comunicaciones telefónicas en el proceso penal español", *Ius Inkarri*, vol. 9, nº 9, (2020), págs. 237–258. https://doi.org/10.31381/iusinkarri.v9n9.3687.

VILÀ CUÑAT, A., "E-evidence: ¿una evidencia?", *Revista Sistema Penal Crítico*, vól. 4 (2023), págs. 1-14.

VRIST RØNN, K., OBELITZ SØE, S., "Is social media intelligence private? Privacy in public and the nature of social media intelligence", *Intelligence and National Security*, vol. 34, nº 3 (2019), págs 362-378. Disponible en: https://doi.org/10.1080/02684527.2019.1553701

JURISPRUDENCIA:

STS 246/1995, de 20 de febrero.

STC 181/1995, de 11 de diciembre

STC 49/1999, de 5 de abril.

STC 123/2002, de 20 de mayo

STS 1932/2008, de 9 de mayo.

STS 513/2010, de 2 de junio

STS 15/2012, 20 de enero.

STC 27/2020, de 24 de febrero.

Caso Rotaru contra Rumanía, STEDH de 4 de mayo de 2000, Sentencia 28341/95.

Caso Segerstedt-Wiberg contra Suecia, STEDH de 6 de junio de 2006, Sentencia 62332/00.

STJUE *Tele2 Sverige AB* contra *post-och telestyrelsen y Secretary of State for the Home Department* contra *Tom Watson* y otros, C-20