IUS ET SCIENTIA
2023 • Vol. 9 • Nº 1• ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023

Ciberpatrullaje en el medio virtual. Delimitando conceptos

CYBERPATROL IN THE CYBERSPACE. DELIMITING CONCEPTS

Manuel Tavora Serra
Universidad de Sevilla
mtavora@us.es 0009-0002-0460-623X

Recibido: 25 de mayo de 2023 | Aceptado: 14 de junio de 2023

RESUMEN

Con el presente trabajo, queremos realizar una aproximación conceptual a la actividad que desarrollan en el medio virtual las Fuerzas y Cuerpos de Seguridad del Estado en cumplimiento de sus funciones de prevención e investigación de los comportamientos delictivos sin control jurisdiccional previo, distinguiendo entre el *ciberpatrullaje*, cuando dicha actividad tiene lugar con carácter previo a un proceso penal, y la *ciberinvestigación*, cuando tiene lugar en el marco de un proceso penal previamente incoado.

PALABRAS CLAVE

Ciberpatrullaje
Ciberinvestigación
Diligencias de investigación tecnológica
Ciberespacio

ABSTRACT

With this article, we want to make a conceptual approach to the activity carried out in the cyberspace by the police forces in compliance with their functions of prevention and investigation of criminal behavior without prior judicial review, distinguishing between *cyberpatrolling*, when such activity takes place prior to a criminal process, and *cyberinvestigation*, when it takes place in the context of criminal proceedings previously initiated.

KEYWORDS

Cyberpatrolling
Cyber investigation
Technological investigation proceedings
Cyberspace

I. Palabras previas

1.1. Delimitación del objeto de estudio

El objeto de este trabajo es el examen de la actividad desarrollada en el medio virtual por las Fuerzas y Cuerpos de Seguridad del Estado en cumplimiento de sus funciones de prevención e investigación de los comportamientos delictivos. En concreto, nos centraremos en los casos en que no existe control jurisdiccional previo, con el fin de verificar si es posible que, en el desarrollo y ejecución de dicha actividad de *ciberpatrullaje* y *ciberinvestigación*, los derechos fundamentales de quienes sean objeto de las mismas (fundamentalmente, quienes ocupen la posición procesal de investigado) resultan afectados.

Dentro del objeto de nuestra investigación, hemos distinguido, por un lado, la actividad de investigación policial que se verifica en un momento anterior a la incoación de un proceso penal –el denominado *ciberpatrullaje*–, y, por otro lado, la actividad de investigación policial que tiene lugar en el marco de un proceso penal ya incoado, pero que continúa sin precisar de autorización judicial previa, que nos hemos atrevido a denominar, en un intento meramente funcional y con el ánimo de diferenciarla de la anterior, como *ciberinvestigación*.

1.2. Trascendencia del objeto de estudio

Ese nuevo medio virtual común, denominado ciberespacio, encuentra sus orígenes en el proyecto ARPANET (*Real Academia de Ingeniería*, 2020). Supone uno de los hitos más trascendentales de nuestra época y, acaso, de nuestra historia, que influye en todos los ámbitos de la existencia individual y social (González Hurtado, 2013, pp. 17-57).

A pesar de los avances que comporta, y en la medida en que los sujetos que actúan en él siguen siendo –por el momento (*Müller and Bostrom AI Progress Poll*, 2014)– los mismos que en la realidad material, las modificaciones e influencias no dejan de suponer sino modalidades de conductas ya existentes con anterioridad. En el medio virtual se verifican, por tanto, unas mismas conductas que en el medio material, pero con variaciones debidas al ambiente en que se desarrollan. De esa manera, y siguiendo la misma lógica expuesta, el *ciberpatrullaje* no deja de ser una modalidad de una actividad bien conocida por la doctrina respecto de las Fuerzas y Cuerpos de Seguridad del Estado –la de prevenir e investigar la comisión de delitos–, que ha debido adaptarse a las particularidades y exigencias del medio virtual.

Ahora bien, la aplicación de las innovaciones tecnológicas a las conductas tradicionales puede aumentar su intensidad y alcance hasta tal punto que pueda entenderse que ha mutado su condición o que, al menos, sea precisa una regulación específica que garantice su encaje en el marco jurídico. Es lo que sucede con la criminalidad y la investigación policial y sus contrapartidas virtuales: el cibercrimen, por un lado, y el ciberpatrullaje y la ciberinvestigación, por otro (Ortiz Pradillo, 2013, pp. 317-319).

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 81-97
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.06

Así, la magnitud cuantitativa y cualitativa de los daños que originan los *ciberdelito*s es innegable, como lo es su potencialidad global para afectar a la economía y el desarrollo tecnológico de todo el mundo(*The Economic Impact of Cybercrime and Cyber Espionage*, 2020). De igual modo, la digitalización de la información y la generación de bases de almacenamiento y tratamiento de datos, suscitan cuestiones en materia de investigación policial a un ritmo que desborda el aparato público, que se encuentra limitado por los tiempos de su propia burocracia. En este contexto, además, la necesidad de responder de manera inmediata a la realidad social ha justificado, en ocasiones, que se admita cierta relajación en determinadas garantías, lo que hace resurgir peligrosamente la idea de que las Fuerzas y Cuerpos de Seguridad pueden infringir los derechos fundamentales para desarrollar con eficiencia y eficacia sus funciones de prevención e investigación(Asencio Mellado, 2019, p. 3).

Lo cierto es que, de manera especialmente destacada en el ámbito del *ciberespacio*, la constante búsqueda de la seguridad nacional por los poderes públicos, persiguiendo una mayor eficiencia en la evitación, persecución y represión de los delitos (en especial, en la lucha contra el terrorismo), parece justificar una creciente actitud invasora en el ámbito de las telecomunicaciones que, consecuentemente, restringe gravemente los derechos fundamentales de los ciudadanos, llegando a apreciarse, incluso, la existencia de una suerte de toque de queda digital (Cabezudo Rodríguez, 2016). En este sentido, existen numerosos ejemplos: el espionaje masivo de las comunicaciones por parte la Agencia de Seguridad Nacional revelado por Snowden, otras redes tradicionales de espionaje internacional de las comunicaciones como *Echelon*; programas para la interceptación de mensajes trasmitidos por correo electrónico, como el *Carnivore* del FBI norteamericano; o, incluso, el proyecto europeo *Enfopol*. A todo ello hay que añadir las coincidentes propuestas o aprobaciones de iniciativas legislativas para dar cobertura a tales prácticas, como la *Patriot Act*, en Estados Unidos o la *Investigatory Powers Act*, en Inglaterra, la Loi relative au renseignement en Francia, o la *Gesetz zur Beschränkung des Brief, Post– und Fernmeldegeheimnisses*, en Alemania.

Todo ello ha dado forma a un nuevo paradigma calificado como de "sociedad del riesgo", en el que se abandona la idea del "Estado del bienestar" para adoptar la del "Estado de la seguridad", con la consiguiente expansión, no ya de la jurisdicción penal –que también–, sino de los poderes investigadores del Estado (Jiménez Mejía, 2014, p. 3). Esta tendencia ha trascendido al modelo económico vigente, llegando a identificarse como capitalismo de la vigilancia (Zuboff, 2019) o capitalismo de control (Lloveras Soler, 2020, p. 10).

II. Algunos conceptos preliminares

2.1. Ciberespacio y ciberdelincuencia

El *ciberespacio* es un medio que surge con la propia existencia de internet, posibilita la conectividad universal y facilita el libre flujo de información, servicios e ideas, estimula

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 81-97
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.06

el emprendimiento y el crecimiento socioeconómico y transforma a escala global los procesos productivos, especialmente con las nuevas herramientas de inteligencia artificial, robótica, *big data*, *blockchain* e *internet of things*.

En relación con las conductas delictivas, el ciberespacio, a su vez, se caracteriza por su inherente ausencia de soberanía, su débil ejercicio de la jurisdicción, la facilidad de acceso a los comportamientos delictivos y la dificultad de atribución de la autoría de las conductas que en él se desarrollan.

La doctrina, apoyándose en estudios realizados por diversas instituciones, ya ha distinguido un doble impacto de la ciberdelincuencia. Por un lado, encontraríamos el coste económico directo y mensurable, computado en función del perjuicio que ocasionara a las víctimas, que ya en 2013 se admitía entre los 100.000 y 500.000 millones de dólares (*The Economic Impact of Cybercrime and Cyber Espionage*, 2020). Por otro lado, incluso con mayor trascendencia a la hora de determinar el impacto real de las formas de ciberdelincuencia en nuestra sociedad, también se atiende a los efectos indirectos, como son las interrupciones de los servicios, la disminución de la confianza de las actividades en línea, el coste de protección de las redes, de seguros y de trabajos de recuperación de ataques informáticos, así como el daño reputacional a la marca de la empresa atacada.

El cibercrimen ya genera más beneficios que el narcotráfico -según refiere Interpol (*La ciberdelincuencia, un gran negocio*, 2022)-, y tiene unos costes que crecen un 15% anual a nivel global. Junto a lo anterior, quizás sería debido reconocer, igualmente, que un nuevo mercado de productos y servicios, el de la seguridad informática, surge por la propia existencia del peligro del cibercrimen y los ciberataques, cifrado en 2023 en 182 mil millones de dólares (*Cybersecurity Market Size & Share Analysis - Industry Research Report - Growth Trends*, 2023).

En España, el Instituto Nacional de Ciberseguridad, ha realizado diversos estudios del estado de la sociedad de la información en el escenario español y los riesgos de ciberseguridad que se detectan (*Guias Y Estudios | INCIBE-CERT | INCIBE*, 2023).

2.2. Prueba electrónica y dato informático

La LO 16/1994, de 8 de noviembre, introdujo la posibilidad, si bien genérica, de utilizar medios técnicos, electrónicos e informáticos en los órganos judiciales, modificando para ello la Ley Orgánica 6/1985, de 1 de julio. Posteriormente, La Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, fue la que de modo expreso incorporó la regulación de las nuevas tecnologías en materia probatoria al proceso (Bonet Navarro, 2020, p. 279). Así, los artículos 382 y 384 regulan la incorporación de información y datos relevantes al proceso a través de la reproducción ante el tribunal de palabras, imágenes y sonidos captados mediante instrumentos de filmación, grabación y similares. Seguidamente, la Ley 18/2011, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, y la Ley 42/2015, de reforma de la LEC, terminaron por consolidar la aplicación de las TICs en la administración de justicia.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 81-97
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.06

En síntesis, por prueba electrónica, informática o digital cabe entender "toda la información de valor probatorio contenida en un medio electrónico o transmitida por dicho medio" (Bonet Navarro, 2020, p. 279). También puede definirse como "aquella información contenida en un dispositivo electrónico a través del cual se adquiere el conocimiento de un hecho controvertido, bien mediante el convencimiento psicológico, bien al fijar este hecho como cierto atendiendo a una norma legal" (Sanchís Crespo, 2012, p. 713).

Por su parte, el concepto de "dato informático" se define en el Convenio de Budapest sobre Ciberdelincuencia de 23 de noviembre de 2001 como "toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función", así como el de "medio electrónico", que se define en el anexo de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, como "mecanismo, instalación, equipo o sistema que permite producir, almacenar o transmitir documentos, datos e informaciones; incluyendo cualesquiera redes de comunicación abiertas o restringidas como internet, telefonía fija y móvil u otras".

Es necesario poner también en correlación estas distinciones con la oportuna diferenciación entre datos de tráfico y datos de abonado. Los primeros pueden definirse como "todos aquellos relativos a la comunicación por medio de sistema informático, generados por el sistema informático que forma parte de la cadena de comunicación, indicando origen, destino, ruta, hora, fecha, tamaño, duración o tipo de servicio subyacente" (Calvo López, 2017, p. 7), mientras que los segundos quedan definidos en el artículo 18.3 del Convenio de Budapest, que indica que por datos de abonado "se entenderá 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 sobre la base de un contrato o de un acuerdo de servicios".

La distinción es fundamental porque la ley y la jurisprudencia vienen considerando los datos de tráfico como parte del proceso comunicativo, quedando por tanto incluidos en la protección dispensada por el artículo 18.3 CE, que establece el monopolio jurisdiccional sobre su limitación. Por el contrario, los datos de abonado, en tanto que no se consideran como parte de un proceso de comunicación, quedan protegidos únicamente por el artículo 18.4 CE, que permite su afección sin necesidad de previa autorización judicial (Calvo López, 2017, p. 8).

No podemos finalizar este capítulo sin hacer una referencia, siquiera breve, a la situación en la que actualmente se encuentra el instituto de la prueba ilícita y la consiguiente regla de exclusión, de acuerdo con la doctrina de nuestro Tribunal Constitucional. Si

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 81-97
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.06

las SSTC 114/1984, de 29 de noviembre, y 85/1994, de 14 de marzo, supusieron hitos fundamentales en el régimen de la prueba ilícita en nuestro país, la STC 97/2019, de 16 de julio, ha supuesto una modificación radical de dicho instituto, declarando que la garantía de ilicitud de las pruebas obtenidas con vulneración de derechos fundamentales no está contenida por sí misma, y de forma autónoma, en el resto de las garantías del artículo 24.2 CE -como debería suceder a consecuencia de la supremacía de los derechos fundamentales en el ordenamiento jurídico- sino que, en realidad, está integrada dentro del concepto de un proceso justo y equitativo. De este modo, la obtención de pruebas con vulneración de derechos fundamentales ha pasado a ser meramente instrumental y únicamente atendible si, además, se entiende vulnerada dicha idea de un proceso justo y equitativo (Asencio Mellado, 2021, p. 192). La consecuencia natural de este giro no puede ser otra que la relajación de la regla de exclusión de la prueba ilícita, al concluir que, en la actualidad, no resulta necesario mantener un estímulo disuasorio de tal magnitud (Armenta Deu, 2020, p. 128).

2.3. Derechos fundamentales

La obtención de la prueba digital afecta a los derechos fundamentales declarados en el artículo 18 CE, esto es, la intimidad personal, el secreto de las comunicaciones, la inviolabilidad domiciliaria (en los supuestos en que el dispositivo electrónico sea hallado en el marco de una entrada y registro en domicilio), y el derecho a la autodeterminación informativa en el ámbito de la protección de datos personales.

El derecho fundamental a la intimidad personal y familiar está reconocido en el artículo 18.1 CE, junto con los derechos fundamentales al honor y a la propia imagen, y también en el artículo 8 CEDH. Su régimen se desarrolla en la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Es un derecho personalísimo, exclusivo de las personas físicas, irrenunciable y que se extingue con el fallecimiento, y tiene una doble dimensión, la personal y la familiar, reconociéndose ambas intimidades como merecedoras de protección, como destacan las SSTC 124/1985, de 17 de octubre y 69/1999, de 26 de abril, y la STS 592/2011, de 12 de septiembre. En según qué circunstancias, sus fronteras respecto de otros derechos fundamentales, como los de no declarar sobre la ideología, religión o creencias propias del artículo 16.2 CE, la inviolabilidad del domicilio del artículo 18.2 CE o el secreto de las comunicaciones del artículo 18.3 CE, pueden quedar difuminadas, como, de hecho, advierte la doctrina (Etxeberria Guridi, 2011, p. 393). En definitiva, protege el ámbito personal y familiar de dignidad de los ciudadanos frente a la acción, el conocimiento y la divulgación de terceros, Como se extrae de las SSTC 231/1988, de 2 de diciembre; 197/1991, de 17 de octubre, 142/1993, de 22 de abril, 57/1994, de 28 de febrero, 98/2000, de 10 de abril, 186/2000, de 10 de julio, 70/2002, de 3 de abril, 218/2002, de 25 de noviembre, 127/2003, de 30 de junio, 23/2007, de 30 de junio o STS 882/2011, de 7 de diciembre.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 81-97
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.06

El derecho a la inviolabilidad del domicilio queda reconocido en el artículo 18.2 CE. En cuanto a su relación con el derecho fundamental a la intimidad, en la STC 94/1999, de 31 de mayo, se ha afirmado que el derecho fundamental a la inviolabilidad domiciliaria protege de forma instrumental la vida privada de una persona (Arrabal Platero, 2019, p. 130)hasta su valoración judicial, pasando por su aportación al proceso a través de los medios de prueba legalmente previstos. Para ello, son objeto de examen las diligencias de investigación, incluyendo aquellas tecnológicas, susceptibles de utilizarse en el proceso penal para la obtención de este tipo de prueba; así como la ilicitud probatoria, en general y la exclusión de la prueba tecnológica, en particular, habida cuenta de la posible vulneración de los derechos fundamentales clásicos (privacidad, secreto de las comunicaciones, inviolabilidad del domicilio. Por lo que se refiere a su contenido, constituye el poder de su titular de impedir la agresión, entrada o permanencia de un tercero en su domicilio, por ser un ámbito reservado a su libertad más íntima. En ese sentido, se ha afirmado que "el domicilio constituye el espacio físico cerrado en el que el individuo puede ejercer su libertad más amplia e íntima, quedando formalmente protegido o inmune frente a toda clase de injerencia externa" (Rives Seva, 2022, p. 55).

El derecho al secreto de las comunicaciones se encuentra reconocido en el artículo 18.3 CE. Este derecho protege el proceso de comunicación que se encuentre en marcha entre dos titulares del mismo, que pueden ser personas físicas o jurídicas, nacionales o extranjeras, tanto en cuanto a su existencia como en cuanto a su contenido, respecto de injerencias de terceros. Sin embargo, una vez que se finaliza la comunicación, la protección constitucional se tiene que realizar a través de otros derechos fundamentales, como el derecho a la intimidad. El criterio para determinar si el secreto de las comunicaciones resulta o no afectado parece ser, por tanto, si los datos de la comunicación a que se accede han sido obtenidos con interferencia o sin interferencia del proceso de comunicación (Vegas Torres, 2015, p. 6).

El derecho fundamental a la protección de datos, también conocido como derecho a la autodeterminación informativa, queda previsto en el artículo 18.4 CE –lo que, habida cuenta del momento histórico en que fue aprobada, es calificado como un hito por la doctrina (Ortega Giménez & González Martínez, 2009)–, y desarrollado por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Se ha definido como "la facultad de toda persona para ejercer control sobre la información personal almacenada en medios informáticos tanto por las administraciones públicas como entidades u organizaciones privadas" (Lucena Cid, 2012). El derecho fundamental en cuestión ya fue abordado por las SSTC 290/2000 y 292/2000, de 30 de noviembre (Arrabal Platero, 2019, p. 165)hasta su valoración judicial, pasando por su aportación al proceso a través de los medios de prueba legalmente previstos. Para ello, son objeto de examen las diligencias de investigación, incluyendo aquellas tecnológicas, susceptibles de utilizarse en el proceso penal para la obtención de este tipo de prueba; así como la ilicitud probatoria, en general y la exclusión de la prueba tecnológica, en particular, habida cuenta de la posible vulneración de los derechos fundamentales clásicos (privacidad, secreto de las comunicaciones, inviolabilidad del domicilio.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 81-97
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.06

Finalmente, debemos referirnos al derecho fundamental al propio entorno virtual. En nuestro ordenamiento jurídico no existe previsión de un derecho fundamental a la privacidad informática que se considere de manera autónoma y diferenciada de la manifestación genérica del derecho a la intimidad (Martín Ríos, 2020, p. 126). En consecuencia, el derecho al propio entorno virtual es un derecho fundamental de creación jurisprudencial y recientísimo origen, concebido para amparar al conjunto de información cibernética que configura el perfil de un ciudadano en particular.

No está previsto explícitamente en nuestro ordenamiento jurídico, sino que ha sido la práctica de nuestros tribunales la que lo ha configurado, sin perjuicio de la silueta que marcan los artículos 588 y siguientes LECrim. En general, este derecho interviene cuando se accede al conjunto de información digital que acumula una persona en su dispositivo personal (Fuentes Soriano, 2020, p. 725).

Generalmente, viene a señalarse como primer reconocimiento del mismo la sentencia del Tribunal Constitucional alemán dictada el 27 de febrero de 2008, en la que, tras comprobar la insuficiencia de la protección que dispensaban frente a investigaciones tecnológicas los derechos fundamentales al libre desarrollo de la personalidad, al secreto de las comunicaciones y a la inviolabilidad del domicilio, reconoció la existencia de un nuevo derecho, que entendió como "el derecho fundamental a la garantía de confidencialidad e integridad de los grupos informáticos", cuyo objeto era "proteger la vida privada y personal de los sujetos de los derechos fundamentales contra el acceso por parte del Estado en el ámbito de las tecnologías de la información, en la medida en que el Estado posea acceso al sistema de tecnologías de la información en su conjunto y no sólo a los acontecimientos de comunicación individuales o a los datos almacenados" (Cabezudo Rodríguez, 2016, p. 42).

III. Actividad autónoma previa al proceso penal

3.1. Delimitación conceptual

En este apartado, es nuestra intención analizar esa actividad de prevención de la criminalidad que, mediante el rastreo de la red y, en general, el uso de la informática, pueden acometer las Fuerzas y Cuerpos de Seguridad del Estado sin necesidad de autorización judicial, sin que exista un destinatario específico de las averiguaciones y, en consecuencia, sin que exista un procedimiento penal incoado. Nos referimos aquí, por tanto, a la actividad de "mantenerse a la escucha" por parte de la policía, en una conducta paralela a la de que aquellos agentes que patrullan físicamente un terreno o territorio, como las calles de una ciudad, lugares con mayor densidad de personas, etc.

En la lucha contra la ciberdelincuencia, la necesidad de conseguir la máxima eficacia y precisión técnica ha obligado tanto a crear grupos especializados dentro de las Fuerzas y Cuerpos de Seguridad nacionales como a la constitución de organismos internacionales expertos en la materia. A nivel nacional, los cuerpos expertos de que disponemos son, por un lado, la Unidad de Investigación Tecnológica de la Policía Nacional y, por otro lado, el Grupo de Delitos Telemáticos de la Guardia Civil.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 81-97
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.06

La doctrina se ha venido refiriendo al *ciberpatrullaje* como aquella actividad de rastreo y sondeo de contenidos que desarrollan habitualmente las Fuerzas y Cuerpos de Seguridad del Estado en el medio *cibernético* abierto en cumplimiento de los fines preventivos e investigativos encomendados por el legislador (este matiz entendemos que es fundamental, habida cuenta de la evidente falta de legislación en materia de *ciberpatrullaje* y demás actividad "autónoma" de la policía o del Ministerio Fiscal). Es decir, se trata de la definición de la actividad de patrullaje tradicional, a la que se le han añadido las modificaciones que el medio virtual requiere.

Como hemos referido, en nuestro ordenamiento jurídico se distinguen, desde una perspectiva general, dos funciones policiales realizadas por los Cuerpos y Fuerzas de Seguridad del Estado: la prevención de la delincuencia, mediante el mantenimiento de la seguridad ciudadana y el orden público, y la investigación de delitos, que es la actividad dirigida a la búsqueda de evidencias que permitan esclarecer los hechos delictivos ya cometidos y que están siendo objeto de investigación (Velasco Núñez, 2010, p. 161). Pues bien, dentro de la primera categoría se encuentra el denominado *ciberpatrullaje*, entendido como el conjunto de actuaciones de vigilancia, prevención y evitación de ilícitos penales llevadas a cabo por la policía en el ámbito del *ciberespacio*.

Dos grandes factores intervienen en la aparición del *ciberpatrullaje* como uno de los principales interrogantes de nuestro tiempo. Por un lado, la denominada *war on terror* (Martínez Santos, 2013), término que se emplea para designar a la política desarrollada desde los atentados del 11S por Estados Unidos y el bloque occidental y que, en plena evolución de la "sociedad del riesgo" (Beck, 2013) y con la inestimable ayuda de la corriente que defiende el "Derecho penal del enemigo" ha provocado que, paulatinamente, se vayan relajando las garantías del Estado de derecho por entender que, en determinados supuestos, el fin justifica los medios. Por otro lado, el hecho de que las herramientas que se utilizan para las actividades de *ciberpatrullaje* –por naturaleza, menos intrusivas que las diligencias de investigación, que precisan de autorización judicial como regla general– son, en realidad, las mismas herramientas que se utilizan para llevar a cabo diligencias de investigación, conservando la potencialidad lesiva del derecho fundamental afectado y presentando como única diferencia el fin al que se las destina en ese momento concreto.

Estas circunstancias nos hacen concluir que es fundamental que se establezcan deberes de transparencia respecto de las herramientas utilizadas y del modo en que lo son. Ejemplo de ello es la iniciativa desarrollada por la *Public Oversight of Surveillance Technology Act*, en Nueva York (POST), que pretende obligar al departamento de policía a publicar información básica sobre las herramientas de vigilancia que utiliza y las medidas de seguridad adoptadas para proteger la libertad y derechos civiles de los ciudadanos (*The Public Oversight of Surveillance Technology (POST) Act*, 2021).

3.2. Escasa previsión normativa

Las Fuerzas y Cuerpos de Seguridad del Estado en el desempeño de sus funciones como Policía Judicial, tienen entre sus atribuciones las de garantizar la seguridad ciudadana,

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 81-97
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.06

averiguar la autoría y circunstancias de los delitos, y recoger los efectos, instrumentos y pruebas de ellos, poniéndolos a disposición de la autoridad judicial. Estas previsiones se establecen en los artículos 104 CE y 549.1 LOPJ.

Pues bien, si la función de averiguación de los delitos y puesta a disposición de sus efectos a la autoridad judicial sí goza de una regulación expresa -y, en especial, respecto de las diligencias de investigación tecnológicas desde la entrada en vigor de la LO 13/2015-, con el *ciberpatrullaje* no sucede lo mismo, no existiendo un cuerpo normativo específico y siendo necesario acudir, por analogía, a la regulación existente acerca del "patrullaje físico", que tampoco es muy abundante. Los preceptos que regulan esta actividad por parte de los Cuerpos y Fuerzas de Seguridad del Estado son los artículos 282 LECrim, 11.1 LOFFCCSS y 22.2 de la LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (vigente conforme a la disposición transitoria de la Ley Orgánica 3/2018, de 5 de diciembre).

En tal sentido se pronunciaba la STC 115/2013: "En segundo término, los agentes policiales actuaron en el presente caso con el apoyo legal que les ofrecen el artículo 282 de la Ley de enjuiciamiento criminal, el artículo 11.1 de la Ley Orgánica 2/1986, de 13 de marzo, de fuerzas y cuerpos de seguridad, y el artículo 14 de la Ley Orgánica 1/1992, de 21 de febrero, sobre protección de la seguridad ciudadana, que conforman "una habilitación legal específica que faculta a la policía para recoger los efectos, instrumentos y pruebas del delito y ponerlos a disposición judicial y para practicar las diligencias necesarias para la averiguación del delito y el descubrimiento del delincuente" (SSTC 70/2002, FJ 10, y 173/2011, de 7 de noviembre, FJ 2). Entre estas diligencias se encuentra la de examinar o acceder al contenido de esos instrumentos o efectos, así como a los documentos o papeles que se le ocupen al detenido, realizando un primer análisis de los mismos, siempre que ello sea necesario de acuerdo con una estricta observancia de los requisitos dimanantes del principio de proporcionalidad (SSTC 70/2002, FJ 10, y 173/2011, FJ 2)."

La ausencia de normativa específica reguladora al respecto es destacable, porque, aunque es cierto que el monopolio jurisdiccional está previsto exclusivamente para cuando se afecta al derecho fundamental al secreto de las comunicaciones y para algunas manifestaciones del derecho a la intimidad, como la inviolabilidad del domicilio, también es cierto que toda injerencia en un derecho fundamental –con independencia de la exigencia de la previa autorización judicial o no– debe estar suficientemente prevista en el ordenamiento jurídico a fin de superar el triple requisito exigido por el artículo 8.2 CEDH. Estos tres requisitos necesarios para que una injerencia en el derecho a la vida privada pueda considerarse legítima son los siguientes: i) que la injerencia esté prevista en la ley, que se identifica con el derecho nacional en una perspectiva material –puede admitirse dentro de dicho concepto los criterios jurisprudenciales asentados; ii) que la injerencia obedezca a uno de los fines legítimos previstos en el artículo 8.2 CEDH: seguridad nacional, seguridad pública, bienestar económico del país, defensa del orden y prevención del delito, protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás; y iii) que la injerencia sea necesaria en una sociedad democrática, elemento este en el que se ubica el principio de proporcionalidad en sentido estricto.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 81-97
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.06

Esta circunstancia, además, no es nueva, sino que ya ha sido puesta de manifiesto por la doctrina hace algún tiempo (Nieva Fenoll, 2008, p. 5), incluso en relación con el patrullaje y las técnicas de investigación "tradicionales", señalándose el olvido casi crónico en que incurre el legislador a la hora de establecer una regulación específica sobre la actividad de investigación, vigilancia, seguimiento y averiguación de la policía y una suerte de asunción espontánea -a nuestro juicio, injustificada- por parte de los agentes policiales y judiciales de que, para mantener la eficacia de dichas actividades, es necesario que el detalle de las mismas permanezca en secreto. Este convencimiento, además, parece amparar no sólo el *modus operandi* en general, sino, incluso, las actividades concretas de investigación previa a la instrucción (patrullaje), en las que parece concluirse -a nuestro juicio, sin suficiente justificación- que es necesario mantener cierto sigilo sobre la actuación policial.

3.3. Manifestaciones del fenómeno

El contenido material del *ciberpatrullaje* puede identificarse con la llamada inteligencia sobre fuentes abiertas, u *open–source intelligence* (OSINT), que es una práctica consistente en recabar datos e información de fuentes disponibles al público con la finalidad de obtener información suficiente sobre una determinada circunstancia, escenario o decisión relacionada con la seguridad nacional, la aplicación del ordenamiento jurídico o, incluso, con la inteligencia de negocios. Su utilidad reside en que, mediante el tratamiento adecuado, permite extraer una funcionalidad no prevista de datos públicamente disponibles, aprovechando las sinergias que pasan desapercibidas al resto de ciudadanos.

La inteligencia sobre fuentes abiertas puede ofrecer resultados muy relevantes en la lucha contra la cibercriminalidad y la protección frente a injerencias extranjeras. Ahora bien, la potencialidad de dichas técnicas provoca que supongan también un grave riesgo para la privacidad de los ciudadanos, pues el acceso y tratamiento de tales datos pueden servir para multitud de fines difíciles de controlar, como trazar perfiles de la ciudadanía, construir sistemas de previsión de riesgo delictivo, etc.

No podemos, además, dejar de hacer referencia al empleo de técnicas de policía predictiva, búsquedas paramétricas en redes p2p, empleo de drones y acceso a imágenes públicas. Todas estas técnicas, además, se apoyan cada vez más en sistemas de inteligencia artificial y tratamiento automatizado de datos.

IV. Actividad autónoma durante el proceso penal

4.1. Facultades de investigación autónoma auténtica

Los poderes de investigación autónomos –en tanto que no precisan de autorización judicial– que han sido conferidos por el legislador a la Policía Judicial con ocasión de la reforma operada por la LO 13/2015 se encuentran recogidos en los ya mencionados artículos 588 *ter* k), 588 *ter* l) y 588 *ter* m) LECrim, y deben acordarse en el marco de un proceso penal debidamente incoado.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 81-97
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.06

La primera de las posibilidades de investigación autónoma consiste en identificar direcciones IP, prevista en el artículo 588 *ter* e. Como se puede apreciar, la propia redacción del artículo no se refiere en sentido expreso a la actividad de obtención de direcciones IP asociadas a una conexión cibernética, sino que, dando ello por sentado, regula la necesidad de que la Policía Judicial deba solicitar a la autoridad judicial que requiera a las entidades obligadas a colaborar los datos necesarios para identificar y localizar al terminal y su usuario (Barrio Andrés, 2018, p. 264).

El fundamento de esta previsión se encuentra en que la dirección IP, por sí sola, no identifica a persona alguna. Su operatividad se pone de manifiesto, únicamente, cuando se interrelaciona esa dirección IP con ciertos datos de identidad conservados por las operadoras de comunicaciones. Es decir, la dirección IP no identifica, pero permite identificar; por lo tanto, su obtención no resultaría extraña a las labores policiales que regula el art. 22.2 de la LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (vigente conforme a la disposición transitoria de la Ley Orgánica 3/2018, de 5 de diciembre), que permite la recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas, pero la identificación final del usuario mediante el cruce de ese dato con los conservados por imposición de la Ley 25/2007, sí precisará de esa autorización judicial.

La segunda de dichas posibilidades consiste en identificar terminales mediante captación de códigos IMSI, IMEI o MAC, prevista en el artículo 588 *ter* l. La averiguación de esos códigos utilizando medios tecnológicos posibilita la identificación del número de teléfono que emplea el sujeto investigado e, incluso, su geolocalización en un punto geográfico relativamente preciso, desde el que esté efectuando la llamada (Delgado Martín, 2018, p. 452). La falta de exigencia de autorización judicial deriva del extendido conocimiento de que los dispositivos utilizados para averiguar estos identificadores no acceden al contenido de las comunicaciones. Sin embargo, resulta de gran importancia destacar que ocurre más bien lo contrario, pues los *IMSI catchers* pueden acceder al contenido de dichas comunicaciones, afectar a la cobertura del aparato, así como a los metadatos, claves de cifrados, datos de geolocalización e, incluso, escribir y acceder datos sobre la memoria del terminal móvil interceptado (Barrio Andrés, 2018, p. 265).

Por último, la policía judicial tiene la facultad también de identificar titulares, terminales o dispositivos de conectividad, prevista en el artículo 588 *ter* m LECrim. Se trata, en realidad, de un supuesto de cesión de datos concernientes a la titularidad o identificación de un dispositivo electrónico –desvinculados de los procesos de comunicación– a favor del Ministerio Fiscal o de la Policía, sin necesidad de autorización judicial, tal y como afirma la LO 13/2015 en su exposición de motivos (Calvo López, 2017, p. 25).

En el marco de esta diligencia de investigación se ha venido planteando cierta problemática entre la Policía Judicial y el Ministerio Fiscal, por una parte, y los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, de otro lado. Esta controversia tiene su origen en el artículo 3 LDCE, que los incluye entre los datos objeto de conservación. El problema surge cuando los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información,

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 81-97
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.06

al recibir las solicitudes de la Policía o del Ministerio Fiscal con apoyo en el artículo 588 *ter* m LECrim, se niegan a facilitarlos y aducen que, en atención a los artículos 3 y 6 LDCE, es necesaria autorización judicial para ello. Generalmente, se considera que la aparente contradicción entre el artículo 588 *ter* m LECrim y el artículo 6 LDCE debe resolverse, en este particular caso, a favor de la primera, por aplicación del criterio *lex posterior derogat anterior* (Barrio Andrés, 2018, p. 268).

4.2. Facultades de investigación autónoma en supuestos de urgencia

Como ya hemos tenido ocasión de exponer, la adopción de medidas de investigación tecnológica exige autorización judicial con carácter previo a su práctica, dado que con ellas se afectan generalmente los derechos fundamentales a la intimidad, propia imagen, inviolabilidad domiciliaria, secreto de comunicaciones y privacidad informática, entre otros.

Sin embargo, no es menos cierto que es posible que la policía adopte dichas medidas de manera anticipada, prescindiendo de autorización judicial habilitante, siempre que exista una situación de urgencia justificada (Velasco Núñez, 2010, p. 273). La cuestión es, claro está, determinar en qué consiste dicha urgencia.

4.3. Principios aplicables en todo caso

En los artículos 588 *bis* a) y siguientes LECrim se contiene el régimen jurídico común a las medidas de investigación tecnológica que, como sabemos, suponen una injerencia en los derechos fundamentales del artículo 18 CE. La propia ubicación sistemática del precepto evidencia que su contenido es de aplicación a todas las medidas de investigación digitales: interceptación de las comunicaciones telefónicas y telemáticas, interceptación de las comunicaciones telefónicas y telemáticas, captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, registro de dispositivos de almacenamiento masivo de información, y registros remotos sobre equipos informáticos, así como medidas de aseguramiento. Esto es necesariamente destacable porque -como hemos expuesto anteriormente- determinaría qué medidas, aun no precisando de autorización judicial, sí deben someterse a los principios previstos en dichos artículos.

Respecto del principio de especialidad, el apartado segundo del artículo 588 *bis* a) LECrim exige que la medida esté relacionada con la investigación de un delito concreto, sin que puedan autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o, incluso, despejar sospechas sin base objetiva. En ese sentido, lo que prohíbe el principio de especialidad es adoptar de manera prospectiva una medida de investigación de naturaleza tecnológica.

Por lo que se refiere al principio de idoneidad, el apartado tercero del artículo 588 *bis* a LECrim dispone que "servirá para definir el ámbito objetivo y subjetivo y la duración de la medida en virtud de su utilidad." En ese sentido, el Tribunal Supremo y el Tribunal Cons-

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 81-97
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.06

titucional han señalado que la medida es idónea cuando: i) parece adecuada a los fines de la instrucción (SSTS 85/2017, de 15 de febrero, 993/2016, de 12 de enero de 2017); ii) permite seguir avanzando en la instrucción (STS 982/2016, de 11 de enero de 2017); iii) y es susceptible de conseguir el objetivo propuesto (STC 207/1996, de 16 de diciembre).

En cuanto a los principios de excepcionalidad y necesidad, el apartado cuarto del artículo 588 *bis* a) dispone que "solo podrá acordarse la medida: a) cuando no estén a disposición de la investigación, en atención a sus características, otras medidas menos gravosas para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho, o b) cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito se vea gravemente dificultada sin el recurso a esta medida." La idea detrás de esta regulación de supuestos alternativos ha sido la de prever escenarios excluyentes entre sí para que, en cualquiera de ellos, pueda entenderse justificado el cumplimiento de ambos principios.

En cualquier caso, una vez superados estos filtros, ha de analizarse la proporcionalidad en sentido estricto. El principio de proporcionalidad se prevé en el apartado quinto del artículo 588 *bis* a, al establecer que "las medidas de investigación reguladas en este capítulo solo se reputarán proporcionadas cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros. Para la ponderación de los intereses en conflicto, la valoración del interés público se basará en la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho".

V. A modo de conclusión

Como podemos comprobar con los apartados anteriores, en la actualidad concurren varios factores en el ámbito de la prevención e investigación de la cibercriminalidad en el espacio:

Por un lado, la importancia del fenómeno de la cibercriminalidad en nuestra sociedad actual y en las agendas de los poderes reguladores es innegable, a la vista de su facilidad de comisión, su amplio ámbito material de actuación, y la relevancia de los intereses a que puede afectar y de las consecuencias económicas que puede tener.

Por otro lado, la búsqueda de una necesaria eficiencia y eficacia que defienda el sistema establecido provoca que se relajen garantías procesales y materiales consolidadas tras décadas de investigación científica y desarrollo social. La creciente complejidad del ámbito virtual provoca que los derechos fundamentales relativos a la intimidad, las garantías del proceso y, en particular, el instituto de la ilicitud de la prueba, representan trabas, lujos prescindibles, cuya relajación se considera conveniente a fin de alcanzar la mayor protección posible frente a la figura de la ciberdelincuencia.

Además, aunque las diligencias de investigación tecnológica, efectuadas en fase procesal, cuentan con previsión legal suficiente al respecto desde la entrada en vigor

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 81-97
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.06

de la Ley Orgánica 13/2015, de 5 de octubre, el ordenamiento jurídico español continúa sin contener previsión suficiente de las diligencias de averiguación y prevención que, con carácter preprocesal, realiza la policía en el ciberespacio (ciberpatrullaje).

Paralelamente, se aprecian tendencias conducentes a establecer la responsabilidad de los prestadores de servicios e intermediarios de internet por los contenidos de los propios usuarios. Esta atribución supondría, en consecuencia, imponerles la obligación de desplegar una diligencia activa, con facultades de revisión de los datos de los usuarios.

De igual modo, se traslada al usuario el acto de otorgar consentimiento a injerencias en su privacidad por el mero hecho de utilizar un servicio determinado. De esta forma, es la propia compañía prestadora de los servicios la que, además de disponer de los datos de conducta de sus usuarios, asume el esfuerzo de patrullar y analizar los mismos y quien traslada a la policía noticia de aquellas conductas o contenidos potencialmente ilícitos.

De esta manera, se puentea el régimen de garantías y exigencias legalmente establecido para proscribir las investigaciones que no vayan dirigidas a un sujeto específico por razones concretas, la actividad de patrullaje se traslada a los propios prestadores del servicio, y se construye un nuevo consentimiento tácito por parte del usuario.

Bibliografía

Armenta Deu, T. (2020). Prueba ilícita y regla de exclusión: Perspectiva subjetiva. *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum, 2020, ISBN 978-84-945088-7-5, págs. 117-140*, 117-140.

Arrabal Platero, P. (2019). *La prueba tecnológica: Aportación, práctica y valoración*. Tirant lo Blanch.

Asencio Mellado, J. M. (2019). La STC 97/2019, de 16 de julio. Descanse en paz la prueba ilícita. *Diario La Ley*, *9499*.

Asencio Mellado, J. M. (2021). La prueba ilícita y su triste destino. *La Administración de Justicia en España y en América, Vol. I*, 175-197.

Barrio Andrés, M. (2018). *Delitos 2.0 Aspectos penales, procesales y de seguridad de los ciberdelitos* (2ª). Wolters Kluwers.

Beck, U. (2013). *La sociedad del riesgo: Hacia una nueva modernidad*. Grupo Planeta Spain.

Bonet Navarro, J. (2020). Apuntes sobre el concepto, obtención, introducción y fiabilidad de la prueba electrónica. *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum, 2020, ISBN 978-84-945088-7-5, págs. 279-298*, 279-298.

Cabezudo Rodríguez, N. (2016). Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal. *I Jornada del Boletín del Ministerio de Justicia: Las reformas del proceso penal*, *2186*, 7-60.

Calvo López, D. (2017, febrero 16). 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 (apartados K) a M) del art. 588 ter de la LECrim). *Jornadas de Especialistas celebradas en el Centro de Estudios Jurídicos de Madrid*. Jornadas de Especialistas celebradas en el Centro de Estudios Jurídicos de Madrid, Madrid.

Cybersecurity Market Size & Share Analysis—Industry Research Report—Growth Trends. (2023). https://www.mordorintelligence.com/industry-reports/cyber-security-market

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 81-97
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.06

Delgado Martín, J. (2018). *Investigación tecnológica y prueba digital en todas las jurisdicciones* (2ª edición actualizada). La Ley.

Etxeberria Guridi, J. F. (2011). La sentencia del TEDH «S. y Marper c. Reino Unido», de 4 de diciembre de 2008, sobre ficheros de ADN, y su repercusión en la normativa española. *Derecho y nuevas tecnologías, Vol. 1, 2011 (Primera parte. Nuevas tecnologías, sociedad y derechos fundamentales), ISBN 978-84-9830-276-9, págs. 393-406*, 393-406.

Fuentes Soriano, O. (2020). La prueba prohibida aportada por particulares: , A la luz de las nuevas tecnologías. *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum, 2020, ISBN 978-84-945088-7-5, págs. 715-744*, 715-744.

González Hurtado, J. A. (2013). *Delincuencia informática: Daños informáticos del artículo 264 del Código penal y propuesta de reforma* [Http://purl.org/dc/dcmitype/Text]. Universidad Complutense de Madrid.

Guias Y Estudios | INCIBE-CERT | INCIBE. (2023). https://www.incibe.es/incibe-cert/publicaciones/guias-y-estudios

Jiménez Mejía, D. (2014). La crisis de la noción material de bien jurídico en el derecho penal del riesgo. *Nuevo Foro Penal*, *82*, 148-176.

La ciberdelincuencia, un gran negocio. (2022). https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbH1czUwMDAytDA3MzRVK0stKs-7Mz7M1MjAyMjAzNAYJZKZVuuQnh1QWpNqmJeYUpwIAuQrogzUAAAA=WKE

Lloveras Soler, J. M. (2020). Capitalismo de control. *Alternativas económicas*, *80*.

Lucena Cid, I. V. (2012). La protección de la intimidad en la era teconlógica: Hacia una reconceptualización. *Revista internacional de pensamiento político*, *7*, 117-144.

Martín Ríos, P. (2020). El alcance del derecho al propio entorno virtual en la valoración de la evidencia digital. *Derecho probatorio y otros estudios procesales: Vicente Gimeno Sendra. Liber amicorum, 2020, ISBN 978-84-945088-7-5, págs. 1259-1270*, 1259-1270.

Martínez Santos, A. (2013). Terrorismo, proceso penal y derechos fundamentales. *Cuestiones constitucionales*, *29*, 459-466.

Müller and Bostrom AI Progress Poll. (2014, diciembre 29). AI Impacts. https://aiimpacts.org/muller-and-bostrom-ai-progress-poll/

Nieva Fenoll, J. (2008). La protección de derechos fundamentales en las diligencias policiales de investigación del proceso penal. *La ley penal: revista de derecho penal, procesal y penitenceiario*, *50*, 81-101.

Ortega Giménez, A., & González Martínez, J. A. (2009). Protección de datos, secreto de las comunicaciones, utilización del correo electrónico por los trabajadores y control empresarial. *Diario La Ley*, *7188*, 1.

Ortiz Pradillo, J. C. (2013). El impacto de la tecnología en la investigación penal y en los derechos fundamentales. En *Problemas actuales de la justicia penal* (pp. 317-343). Colex.

Real Academia de Ingeniería. (2020). http://diccionario.raing.es/es/lema/arpanet

Rives Seva, A. P. (2022). *La prueba en el proceso penal. Doctrina de la Sala Segunda del Tribunal Supremo.*

Sanchís Crespo, C. (2012). La prueba en soporte electrónico. *Las tecnologías de la información y la comunicación en la administración de justicia: análisis sistemático de la Ley 18/2011, de 5 de julio, 2012, ISBN 978-84-9903-947-3, págs. 707-734*, 707-734.

The Economic Impact of Cybercrime and Cyber Espionage. (2020). https://www.csis.org/analysis/economic-impact-cybercrime-and-cyber-espionage

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 1 • pp. 81-97
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.06

The Public Oversight of Surveillance Technology (POST) Act: A Resource Page. (2021). Brennan Center for Justice. https://www.brennancenter.org/our-work/research-reports/public-oversight-surveillance-technology-post-act-resource-page

Vegas Torres, J. (2015). Sobre el alcance del secreto de las comunicaciones. *Una filosofía del derecho en acción: homenaje al profesor Andrés Ollero, 2015, ISBN 978-84-7943-489-2, págs. 1609-1626*, 1609-1626.

Velasco Núñez, E. (2010). *La investigación de delitos cometidos a través de Internet y otras nuevas tecnologías: Cuestiones procesales* [Http://purl.org/dc/dcmitype/Text]. Universidade da Coruña.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 1 • pp. 81-97
ISSN 2444-8478 • https://doi.org/10.12795/IESTSCIENTIA.2023.i01.06