UNIVERSITAT DE BARCELONA

Investigación y prueba del ciberdelito

Josefina Quevedo González

Programa de Doctorado en Derecho y Ciencia Política
Línea de Investigación: Derecho procesal

INVESTIGACIÓN Y PRUEBA DEL CIBERDELITO

Director: Dr. FRANCISCO ORTEGO PÉREZ.
Profesor titular de Derecho Procesal de la Universidad de Barcelona.

Tutor: Dr. DAVID VALLESPÍN PÉREZ.
Catedrático de Derecho Procesal de la Universidad de Barcelona.

JOSEFINA QUEVEDO GONZÁLEZ.

BARCELONA, 2017

RESUM.- S'examina en aquest treball la transcendència que té l'ús d'internet en la aparició de nous delictes i de noves formes de comissió dels il·lícits tradicionals. A tots ells se'ls anomena *ciberdelictes*, la investigació i prova dels quals exigeixen l'adopció d'especials precaucions per a evitar que es frustri la tasca investigadora o es vulnerin drets fonamentals. Per això, s'estudien qüestions bàsiques que susciten els ciberdelictes, com la competència per a conèixer d'aquests, els conflictes de jurisdicció entre Estats, la cooperació internacional i els subjectes especialitzats en la investigació amb especial referència als Equips Conjunts d'Investigació així com a les obligacions a que venen subjectes les empreses proveïdores d'internet. S'analitza la regulació legal de les mesures d'investigació tecnològica necessàries per a la investigació del ciberdelicte, en concret: l'obtenció d'una IP, la identificació de terminals, de dades desvinculades dels processos de comunicació, l'ordre de conservació de dades, la cessió de dades de tràfic, la intercepció de les comunicacions telefòniques i telemàtiques, el registre de dispositius informàtics d'emmagatzemat massiu, el registre remot d'equips, l'agent encobert informàtic i què succeeix amb les trobades casuals descobertes després d'aquestes mesures. Així mateix, es detalla com han de practicar-se aquestes mesures d'investigació amb totes les garanties per a superar el judici de licitud i el de fiabilitat i d'aquesta manera servir de prova davant dels tribunals a l'igual que la resta de les proves informàtiques. Per últim, es dedica un capítol a la valoració judicial de les proves informàtiques segons el principi d'apreciació en consciència contingut a l'art. 741 LECrim i la profusa jurisprudència en la matèria.

RESUMEN.- Se examina en este trabajo la trascendencia que tiene el uso de internet en la aparición de nuevos delitos y de nuevas formas de comisión de los ilícitos tradicionales. A todos ellos se denomina *ciberdelitos,* cuya investigación y prueba exigen la adopción de especiales precauciones para evitar que se frustre la labor investigadora o se vulneren derechos fundamentales. Por ello, se estudian cuestiones básicas que suscitan los ciberdelitos como la competencia para conocer de los mismos, los conflictos de jurisdicción entre Estados, la cooperación internacional y los sujetos especializados en la investigación con especial referencia a los Equipos Conjuntos de Investigación así como a las obligaciones a las que vienen sujetas las empresas proveedoras de internet. Se analiza la regulación legal de las medidas de investigación tecnológica necesarias para la investigación del ciberdelito, en concreto: la obtención de

una IP, la identificación de terminales, de datos desvinculados de los procesos de comunicación, la orden de conservación de datos, la cesión de datos de tráfico, la interceptación de las comunicaciones telefónicas y telemáticas, el registro de dispositivos informáticos de almacenamiento masivo, el registro remoto de equipos, el agente encubierto informático y qué sucede con los hallazgos casuales descubiertos tras estas medidas. Asimismo, se detalla cómo han de practicarse estas medidas de investigación con todas las garantías para superar el juicio de licitud y el de fiabilidad y de esta manera servir de prueba ante los tribunales al igual que el resto de las pruebas informáticas. Por último, se dedica un capítulo a la valoración judicial de las pruebas informáticas según el principio de apreciación en conciencia contenido en el artículo 741 LECrim y la profusa jurisprudencia en la materia.

ABSTRACT.- This paper examines the importance of the use of the Internet in the emergence of new crimes and new forms of commission of traditional illicit. All of them are called cybercrimes, whose investigation and proof require the adoption of special precautions to avoid the frustration of research or fundamental rights violations. For this reason, there is a study of basic issues that are raised by cybercrime, such as the judicial competence to learn about them, conflicts of jurisdiction between States, international cooperation and specialized researching subjects with special reference to Joint Investigation Teams as well as to the obligations to which the internet service providers (ISP) are subject. The legal regulation of the technological research measures necessary for the investigation of cybercrime is analyzed and, in particular: the obtaining of an IP, the identification of terminals, data unrelated to the communication processes, the data preservation order, the cession of traffic data, interception of telephone and telematic communications, search of mass storage devices, remote search of equipment, undercover agent and what happens with casual findings discovered after these measures. It is also detailed how these investigative measures should be practiced with all the guarantees to overcome the legal and reliability trial and thus serve as evidence in court as well as the rest of the computer evidence. Finally, a chapter is devoted to the judicial assessment of computer evidence according to the principle of appreciation in conscience contained in article 741 LECrim and the profuse jurisprudence in the matter.

INDICE GENERAL

INTRODUCCIÓN. 9

ABREVIATURAS. 15

GLOSARIO DE TÉRMINOS TÉCNICOS 21

PRIMERA PARTE

EL CIBERDELITO: ASPECTOS GENERALES Y CUESTIONES TÉCNICAS BÁSICAS. 29

CAPÍTULO PRIMERO

INTERNET Y LA CRIMINALIDAD. 31

1. ORIGEN Y EVOLUCIÓN DE INTERNET Y DE LOS DELITOS VINCULADOS. 31
1.1 La denominada etapa militar. 32
1.2 La denominada etapa académica. 34
1.3 La denominada etapa comercial. 35
1.4. La denominada etapa social. 37

2. FACTORES DE INTERNET QUE FAVORECEN LA COMISIÓN DE LOS DELITOS. 39
2.1 Nociones básicas de internet. 39
2.1.A) Características técnicas. 39
2.1.B) Componentes técnicos. 44
2.1.C) Aplicaciones y servicios. 45
2.2 Internet y el cambio en la concepción tradicional del delito. 48

CAPÍTULO SEGUNDO

CONCEPTO DE CIBERDELITO, CLASES Y TÉCNICAS DE COMISIÓN. 55

1. APROXIMACIÓN AL CONCEPTO. 55

2. CLASIFICACIÓN DE LOS CIBERDELITOS. 59
2.1 Clasificación doctrinal 59
2.2 Clasificación institucional. 65
2.3 Clasificación normativa. 67

3. TÉCNICAS DE COMISIÓN DE LOS CIBERDELITOS. 75

CAPÍTULO TERCERO

JURISDICCIÓN Y COMPETENCIA. 85

1. COMPETENCIA EN RELACIÓN CON LOS CIBERDELITOS COMETIDOS EN TERRITORIO ESPAÑOL Y PARCIAL O TOTALMENTE FUERA DEL TERRITORIO ESPAÑOL. 85

2. LOS CONFLICTOS DE JURISDICCIÓN ENTRE DOS O MÁS ESTADOS PARA INVESTIGAR LOS CIBERDELITOS COMETIDOS EN PARTE FUERA DE SUS RESPECTIVOS TERRITORIOS. 93

CAPÍTULO CUARTO

INSTRUMENTOS DE COOPERACIÓN INTERNACIONAL EN MATERIA DE CIBERDELINCUENCIA. 99

1. ASISTENCIA JUDICIAL..... 99
2. RECONOCIMIENTO MUTUO. 105
3. ENTREGA Y EXTRADICIÓN. 107

SEGUNDA PARTE

LA INVESTIGACIÓN Y PRUEBA EN LOS CIBERDELITOS . 109

CAPÍTULO QUINTO

SUJETOS Y ÓRGANOS DE LA INVESTIGACIÓN DE LOS CIBERDELITOS. 111

1. FISCALES DE CRIMINALIDAD INFORMÁTICA..... 112
1.1 Fiscal de Sala Coordinador para la Criminalidad Informática. 113
1.2 Las Secciones de Criminalidad Informática de las Fiscalías. 114

2. FUERZAS Y CUERPOS DE SEGURIDAD DEL ESTADO ESPECIALIZADAS EN LA LUCHA CONTRA LOS CIBERDELITOS..... 116
2.1 Unidad de Investigación Tecnológica del Cuerpo Nacional de Policía (UIT)..... 117
2.2 Grupo de Delitos Telemáticos de la Guardia Civil (GDT) 118

3. LOS EQUIPOS CONJUNTOS DE INVESTIGACIÓN (JIT)..... 120

4. LAS EMPRESAS PROVEEDORAS DE INTERNET (ISP). 125

5. OTROS ORGANISMOS VINCULADOS A LA PREVENCIÓN Y REPRESIÓN DE LA CIBERDELINCUENCIA 132
5.1 Organismos europeos: 132
5.2 Organismos nacionales:..... 133
5.3 Entidades del tercer sector (Asociaciones, ONGs Y Fundaciones) que son actores relevantes en la labor de prevención y represión de la ciberdelincuencia. 136

CAPÍTULO SEXTO

DERECHOS Y LIBERTADES QUE RESULTAN AFECTADOS. 137

1. EL DERECHO A LA INTIMIDAD. 140
1.1 Requisitos para la injerencia. 142
1.1.A) La Autorización Judicial. 144
1.1.B) Consentimiento del afectado. 147
1.1.C) Intervención policial por razones de urgencia y necesidad. 150

2. SECRETO DE LAS COMUNICACIONES. 154
2.1 Contenido de la comunicación. 154
2.2 Fases del proceso de comunicación a través de una red. 158
2.3 Régimen jurídico del secreto a las comunicaciones. 161

3. EL DERECHO A LA PROTECCIÓN DE DATOS 162

4. EL DENOMINADO "DERECHO A LA IDENTIDAD VIRTUAL." 165

CAPÍTULO SÉPTIMO

TÉCNICAS DE INVESTIGACIÓN DE LOS CIBERDELITOS. 169

1. LAS NUEVAS TÉCNICAS DE INVESTIGACIÓN TECNOLÓGICA. 169

2.TÉCNICAS DE INVESTIGACIÓN TECNOLÓGICA QUE NO PRECISAN AUTORIZACIÓN JUDICIAL. 173
2.1 Obtención de una IP. 173
2.2 Identificación de IMEI, IMSI y MAC. 176
2.3 Obtención de datos desvinculados de los procesos de comunicación. 180
2.3.A) Identificación de titulares o terminales o dispositivos de conectividad. 180
2.3.B) Acceso a datos no integrados en un proceso de comunicación (agenda de un teléfono móvil). 183
2.4 La Orden de Conservación de Datos. 185
2.4.A) Concepto de Datos Informáticos. 185
2.4.B) Régimen jurídico de la Órden de Conservación de Datos. 188
2.5 Captación de Conversaciones Públicas. 193
2.6 Actuación en casos de urgencia. 194

3. TÉCNICAS DE INVESTIGACIÓN TECNOLÓGICA QUE REQUIEREN AUTORIZACIÓN JUDICIAL. 197
3.1 Orden en relación con la cesión de datos sobre tráfico almacenados. 197
3.1. A) Régimen jurídico de la cesión de datos. 197
3.1.B) Procedimiento de cesión de datos conservados. 204
3.1.B. 1) Solicitud de cesión de datos. 204
3.1.B. 2)Resolución judicial. 205

3.2 La interceptación de las comunicaciones telemáticas como vía de investigación criminal de los ilícitos que se cometen a través de la red. 209
3.2.A) Marco Jurídico. 209
3.2.B) Ambito de aplicación de la interceptación de las comunicaciones. 212
1) Medios de Comunicación objeto de Intervención: 214
a) Correo Electrónico. 214
b) SMS y MMS. 221
c) Mensajería Instantánea y las comunicaciones VoIP. 222
d) Redes Sociales. 224
2)Terminales objeto de intervención. 228
a) Identificación del terminal. 228
b) Titularidad del terminal. 231
3) Revelación por un comunicante. 235
4) Comunicante accidental. 237
3.2.C) Procedimiento para intervenir las comunicaciones. 240
1) Resolución Judicial. 241
2) Duración y prórroga. 244
3) Control y cese de la medida. 245

3.3. El registro de dispositivos de almacenamiento masivo de la información. 248
3.3.A) Naturaleza jurídica de los dispositivos informáticos. 248
3.3.B) Autorización requerida en función de su ubicación. 252
3.3.C) Contenido de la resolución judicial y práctica del registro. 256

3.4. Registro remoto sobre equipos informáticos. 263
3.4.A) Presupuestos para su adopción. 266
3.4.B) Duración y deber de colaboración. 270

3.5 El agente encubierto informático. 272

3.6 Hallazgo casual. 284
3.6.A) La doctrina del hallazgo casual en la jurisprudencia. 284
a) Hallazgo casual tras la práctica de un registro domiciliario. 285
b) Hallazgo casual en escuchas telefónicas. 287
c) Diferencias del hallazgo casual descubierto en un registro al descubierto en una intervención telefónica. 288
3.6.B) La regulación del hallazgo casual en la LECrim. 291

CAPÍTULO OCTAVO.

LA PRUEBA DE LOS CIBERDELITOS. 299

1. NATURALEZA JURÍDICA DE LA PRUEBA DE LOS CIBERDELITOS. 299

2. REQUISITOS DE ADMISIBILIDAD DE LAS PRUEBAS INFORMÁTICAS: JUICIO DE LICITUD Y JUICIO DE FIABILIDAD. 307
2.1 Juicio de Licitud. 309
2.1.A) Requisitos para la licitud de la prueba: 310
2.1.B) Consecuencias de la falta de licitud. 312

2.2 Juicio de fiabilidad. 313
2.2.A) *Requisitos técnicos para la captación del IMSI e IMEI.* 315
2.2.B) *Requisitos técnicos para incorporar datos electrónicos de tráfico o asociados.* 316

2.2.C) *Requisitos técnicos para interceptar comunicaciones.* 317
2.2.D) *Requisitos técnicos para los registros de dispositivos.* 333
2.2.E) *Requisitos técnicos para el registro remoto.* 342
2.2.F) *La fiabilidad del agente encubierto informático.* 344
2.2. G) *Consecuencias de la falta de fiabilidad.* 345

3. LA PRUEBA PERICIAL INFORMÁTICA. 348

4. INCORPORACIÓN AL PROCESO DEL MATERIAL PROBATORIO INFORMÁTICO. 356
4.1 Consideraciones generales. 356
4.2 Aportación de la prueba informática por las partes. 368

5. VALORACIÓN DE LA PRUEBA INFORMÁTICA. 370
5.1 Valoración de la prueba documental informática. 370
5.2 Valoración de la Prueba Pericial Informática. 378
5.3 Valor de la Prueba irregular y valor de la prueba ilícita. 385

CONCLUSIONES 399

APÉNDICE NORMATIVO 411

1. NORMATIVA DE ÁMBITO INTERNACIONAL. 413
1. 1. Convenio sobre Ciberdelicuencia. 414

2. NORMATIVA DE ÁMBITO EUROPEO. 417
2.1 Directiva 2000/31/Ce del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados Aspectos Jurídicos de los Servicios de La Sociedad de La Información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico). 418
2.2 Decisión Marco del Consejo, de 28 de Mayo de 2001, Sobre La Lucha Contra el Fraude y la Falsificación de Medios de Pago Distintos del Efectivo. 418
2.3 Directiva 2002/58/Ce Del Parlamento Europeo y del Consejo de 12 de Julio de 2002, relativa al Tratamiento de Datos Personales y a la Protección de la Intimidad en el Sector de las Comunicaciones Electrónicas. (Directiva Sobre la Privacidad y las Comunicaciones Electrónicas). 418
2.4 Directiva 2006/24/Ce del Parlamento Europeo y del Consejo Sobre la Conservación de Datos Generados o Tratados en Relación con la Prestación de Servicios De Comunicaciones Electrónicas de Acceso Público o de Redes Públicas de Comunicaciones. 419
2.5 Directiva 2011/93/UE, Relativa a la Lucha contra los Abusos Sexuales y la Explotación Sexual de los Menores y la Pornografía Infantil. 420
2.6 Directiva 2012/29/Ue del Parlamento y del Consejo, de 25 De Octubre De 2012, por la que se Establecen Normas Mínimas Sobre Los Derechos, El apoyo y la Protección De Las Víctimas De Delitos. 420
2.7 Directiva 2013/40, relativa a los Ataques contra los Sistemas de Información .. 421
2.8 Directiva 2014/41/UE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal. 421
2.9 Reglamento Europeo de Protección de Datos (Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016). 424

2.10 Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016. 424

3. LEGISLACIÓN NACIONAL..... 425
3.1 La Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. 425
3.2 Ley de Enjuiciamiento Criminal. 427
3.3 La Ley 25/2007, De 18 De Octubre, de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones. 429
3.4 La Ley 9/2014, de 9 de mayo (BOE 10 de mayo), General de Telecomunicaciones. 438
3.5 La Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal..... 443

APÉNDICE JURISPRUDENCIAL 447

BIBLIOGRAFÍA 465

INTRODUCCIÓN.

El desarrollo de las tecnologías de la información y la generalización en el uso de las mismas ha tenido reflejo en la delincuencia y la criminalidad, pues la aparición de nuevos tipos delictivos y nuevas modalidades en la comisión de los delitos tradicionales determina que sean cada vez más numerosos los bienes jurídicos objeto de protección penal que pueden verse comprometidos por quienes utilizan los avances de la ciencia para llevar a efecto sus criminales propósitos. Estos cambios en la delincuencia ordinaria han convertido a la ciberdelincuencia en un reto significativo y merecedor de una respuesta legislativa adecuada.

Internet y las redes telemáticas traen consigo un nuevo concepto superador del tradicional de delito informático, el de *ciberdelito*, término internacionalmente acuñado tras el convenio sobre ciberdelincuencia del año 2001. Cuando se habla de ciberdelito se hace referencia a un tipo de delito, ya sea tradicional o propio de la sociedad de la información, propiciado por las tecnologías que ésta aporta, fundamentalmente internet.

Este tipo de conductas ilícitas que se planifican y ejecutan aprovechando las ventajas que ofrecen las nuevas tecnologías de la sociedad de la información, presentan a los efectos de su investigación y/o enjuiciamiento, singularidades y dificultades para su descubrimiento y persecución, así como para la identificación de las personas responsables de estos comportamientos ilícitos. No obstante, el desarrollo de las nuevas tecnologías, además de fomentar las posibilidades al alcance del delincuente, también proporciona poderosas herramientas de investigación a los poderes públicos. Surge así la necesidad de encontrar un delicado equilibrio entre la capacidad del Estado para hacer frente a una fenomenología criminal de nuevo cuño y el espacio de exclusión que nuestro sistema constitucional garantiza a cada ciudadano frente a terceros.

En definitiva, con la aparición del ciberdelito el Derecho Penal se enfrenta a una criminalidad progresivamente más lesiva, que requiere a su vez los necesarios instrumentos procesales para hacerle frente.

Los objetivos que se pretenden con este trabajo son, de una parte, delimitar el concepto de este tipo de delito y su regulación actual, sustantiva y procesal, y de otra, determinar cómo dirigir la investigación, estudiando los métodos principales de

investigación u obtención de pruebas, los datos relevantes en la investigación del hecho e identificación del responsable y cómo obtener los mismos con todas las garantías y respeto a los derechos fundamentales para que pueda ser valorados como prueba sin el menor atisbo de falta de licitud o fiabilidad del material probatorio.

Por ello, divido sistemáticamente este estudio en dos grandes apartados:

A) El primero, dedicado a los aspectos generales y a las cuestiones técnicas básicas del ciberdelito, compuesto por cuatro capítulos en los que se abordan las cuestiones más generales, cuyo conocimiento se hace preciso para profundizar después en las cuestiones relativas a la investigación y prueba.

El primer capítulo introduce la materia objeto de estudio presentando unas nociones básicas del funcionamiento de internet y de la evolución experimentada en las últimas décadas y cómo ha influido esta evolución en la ciberdelincuencia.

El segundo capítulo intenta establecer un concepto de ciberdelito, analizando todas las clasificaciones aportadas por la doctrina, las instituciones y las normas para finalmente tratar las diversas técnicas usadas por los ciberdelincuentes para cometer estos ilícitos.

Los capítulos tercero y cuarto se centran respectivamente en la competencia judicial y la cooperación internacional, claves en la materia pues muchos de los obstáculos que surgen en la investigación de los ciberdelitos derivan de su carácter transfronterizo. Por su propia naturaleza y características, frecuentemente se desarrollan y/o producen efectos en distintos territorios por lo que es importante determinar la competencia en relación con los ciberdelitos cometidos en territorio español y parcial o totalmente fuera del territorio español, y los conflictos de jurisdicción cuando dos o más estados pueden investigar y procesar al mismo autor por ciberdelitos cometidos en parte fuera de sus respectivos territorios. También la tan necesitada cooperación internacional dado que el carácter transnacional de los ciberdelitos hace que en muchos casos sea necesario acudir a instancias internacionales para investigar los rastros dejados en el entorno informático, telemático o virtual o para solicitar alguna diligencia necesaria para el aseguramiento de las pruebas.

B) La segunda parte de la tesis analiza en primer lugar los sujetos especializados a quienes les incumbe la investigación de este tipo de delitos o desempeñan algún papel relevante en la misma y qué derechos fundamentales resultan afectados en la investigación de estos delitos para acto seguido hacer un estudio exhaustivo de las técnicas de investigación tecnológica reguladas en la Ley de Enjuiciamiento Criminal, introducidas en la reforma operada por la *Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.* Esta reforma ha influido decisivamente en la materia objeto de estudio pues viene a dar solución a muchas de las cuestiones que se plantean en la investigación del ciberdelito, mediante la regulación expresa de específicas técnicas de investigación tecnológica, bajo el enunciado que sirve de nueva rúbrica al Título VIII del Libro II de la Ley de Enjuiciamiento Criminal *"De las medidas de investigación limitativas de los derechos reconocidos en el art. 18 de la Constitución"*.

Se intenta establecer una exposición clara y concisa de las técnicas de investigación tecnológica relacionadas con la investigación del ciberdelito. Se clasifican, siguiendo el orden lógico de la investigación, entre las que puede practicar la policía por si misma y que no requieren autorización judicial y aquéllas que sí lo requieren. Dentro de estas últimas, se estudian en primer lugar todas aquéllas que venían practicándose, pese a estar carentes de regulación en LECrim, amparadas en otras leyes y en la jurisprudencia, para finalmente tratar aquéllas que tienen una regulación *ex novo*.

El último capítulo se dedica a la prueba informática. Tras dejar constancia de la naturaleza de estas pruebas se aborda el **doble juicio** al que deben someterse para su admisibilidad: ***a)*** de una parte, el juicio de licitud, que exige que la prueba se haya obtenido sin violar derechos fundamentales, pues en otro caso sería nula (art. 11.1 LOPJ); y ***b)*** de otra, el juicio de fiabilidad, que consiste, como se verá, en examinar la autenticidad (no manipulación) y la integridad (conservación del contenido) del material aportado, la intangibilidad e inalterabilidad del mismo, la ausencia de mala fe y sin técnicas espurias en la obtención de la información recabada en el curso de tal medio de investigación, pues las dudas sobre la fiabilidad determinarán su ineficacia probatoria.

Se analiza la forma de incorporar el material probatorio al acto del plenario y se hace referencia a su valoración judicial según el principio de apreciación en conciencia contenido en el artículo 741 LECrim.

Para finalizar, se añaden un apéndice normativo y otro jurisprudencial al objeto de facilitar el estudio y comprensión de la materia.

La **metodología** seguida ha sido la tradicional en la elaboración de una tesis doctoral de esta disciplina. En una primera fase, se inició por la recopilación de la bibliografía más relevante, su análisis y clasificación. Estas tareas condujeron a la necesidad de una segunda búsqueda bibliográfica, esta vez más selectiva, a la par que jurisprudencial. A partir de aquí, se elaboró una provisional tabla de los posibles contenidos ordenada en función de las ideas sugeridas por los materiales enunciados y una primera redacción de los mismos. Siguiendo las directrices y consejos del director se ha ido puliendo el contenido, se ha dado nueva forma a su organización original hasta llegar a una redacción que puede considerarse definitiva. Paralelamente a todo este proceso se ha realizado una tarea continua de actualización, incorporando de esta manera los nuevos títulos bibliográficos que han ido surgiendo, así como la jurisprudencia que se ha ido dictando en la materia. Finalmente, se ha procedido a la redacción de las conclusiones, al hilo de lo cual se han corregido errores del texto para finalizar con la elaboración de la introducción del trabajo, que recopila y explica, de manera sintética, la obra realizada.

ABREVIATURAS.

ADSL: Acrónimo de la expresión en inglés *Asymmetric Digital Subcriber Line* (línea de abonado digital asimétrica).

AEPD: Agencia Española de Protección de Datos.

ARPA: *Advanced Research Projects Agency*, Agencia de Proyectos de Investigación Avanzada (cambió su nombre a *Defense Advanced Research Projects Agency).*

ARPANET: *Advanced Research Projects Agency Network* (red informática de la Agencia de Proyectos de Investigación Avanzada).

Art: Artículo.

CE: Constitución Española.

CEDH: Convenio Europeo de Derechos Humanos.

CP: Código Penal.

CSC: Convenio sobre ciberdelincuencia.

DARPA: *Defense Advanced Research Projects Agency* (Agencia de Proyectos de Investigación Avanzados de Defensa).

DNS: *Domain Name System* (nombres de dominio).

EDITES: Equipos de Investigación Tecnológica de la Guardia Civil.

ENISA: acrónimo del inglés *the European Union Agency for Network and Information* Security (Agencia Europea para la red y la seguridad de la información).

FNC: *Federal Networking Council* (Consejo Federal de Redes).

FTP: *File Transer Protocol* (protocolo de transferencia de archivos).

GDT : Grupo de Delitos Telemáticos de la Guardia Civil.

HTTP: *Hyper Text Transfer Protocol.*

ICANN: *Internet Corporation for Assigned Names and Numbers.* Organismo que suministra las IP y los nombres de dominio.

IP: *Internet Protocol.*

ISP: *Internet service provider* (Proveedores de acceso o servicios de internet).

JIT: *Joint Investigation Team* (Equipo Conjunto de investigación).

LAJ: Letrado de la Administración de Justicia.

LAN: *local area network.*

LCD: Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

LEC: Ley de Enjuiciamiento Civil.

LECrim: Ley de Enjuiciamiento Criminal.

LGT: Ley General de Telecomunicaciones.

LPM: Ley Procesal Militar.

LO: Ley Orgánica.

LOPD: Ley Orgánica de Protección de datos de carácter personal.

LOPJ: Ley Orgánica del Poder Judicial.

LUTICAJ: Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.

MAC: *Media Acces Code.*

NCP: *Network Control Protocol* (protocolo distribuido, protocolo de control de red).

NSF: *National Science Fundation* (Fundación Nacional para la Ciencia).

NSFNET: *National Science Foundation Network* (red de la Fundación Nacional para la Ciencia).

NU: Naciones Unidas.

OEDE: Orden Europea de Detención y Entrega.

OEI: Orden Europea de Investigación en materia penal.

SMTP: *Simple Mail Transfer Protocol*.

STC: Sentencia del Tribunal Constitucional.

STEDH: Tribunal Europeo de Derechos Humanos.

STJUE: Sentencia del Tribunal de Justicia de la Unión Europea.

STS: Sentencia del Tribunal Supremo.

TC: Tribunal Constitucional.

TCP/IP: *Transmission Control Protocol/Intenet Protocol* (Protocolo de Control de Transmisión y el Protocolo de Internet).

TEDH: Tribunal Europeo de Derechos Humanos.

TIC: Tecnologías de la información y de la comunicación.

TJUE: Tribunal de Justicia de la Unión Europea.

TLD: *Top Level domain* (dominios de nivel superior).

TMT: Tribunal Militar Territorial.

TS: Tribunal Supremo.

UCO: Unidad Central Operativa de la Guardia Civil.

UE: Unión Europea.

UDP: *User Datagram Protocol.*

UIT: Unidad de Investigación Tecnológica de la Policía Nacional.

VPN: *virtual private network* (red privada virtual).

WAIS: *Wide Area Information Server* (servidor de información de área amplia).

GLOSARIO DE TÉRMINOS TÉCNICOS

Para una mejor comprensión adjunto un glosario de los términos técnicos más frecuentemente utilizados, dado el obligado recurso al lenguaje tecnológico.

- Ancho de banda: es una medida de recursos disponibles para transmitir datos. También se usa para definir la velocidad de Internet o la velocidad de conexión.

- *Backup*: copia de seguridad.

- Blog: página en internet que se actualiza de forma periódica para la expresión de pensamientos u opiniones que suele adoptar el formato de un diario personal.

- Buscador: es una herramienta que permite buscar páginas en internet referidas a un tema específico o relacionado con ciertas palabras clave.

- Cliente/Servidor (Client/Server): el modelo cliente-servidor es el sistema de organización de las conexiones entre ordenadores que se utiliza en internet, y en general en todas las redes de ordenadores. Se basa en la clasificación de los ordenadores de la red en dos categorías: las que actúan como servidores (oferentes de información) y otras que actúan como clientes (receptores de información).

- *Cloud*: la "nube" es una metáfora empleada para hacer referencia a determinados servicios que se utilizan a través de internet, que facilita la utilización de recursos desde un lugar remoto.

- Correo no deseado o *SPAM*: correo que no solicitado y que suele tener un remitente desconocido con la finalidad de promover una página web o un determinado producto.

- Dirección IP: es un número identificativo y único de cada dispositivo que se conecta a internet .

- DNS (Domain Name System/Server, servidor de nombres de dominios): sistema de ordenadores que se encarga de convertir las direcciones electrónicas de internet (como http://www.mde.es) en la dirección IP correspondiente y viceversa. Componen la base del funcionamiento de las direcciones electrónicas en Internet. El

sistema DNS está organizado jerárquicamente. Por ejemplo, en España, la gestión de todos los nombres de dominio bajo el dominio de primer nivel ".es" corresponde a la Entidad Pública Empresarial Red.es dependiente del Ministerio de Industria.

- Dominio: es un término empleado en el mundo de internet para referirse al nombre que sirve para identificar direcciones de computadoras conectadas a internet. (Por ejemplo: www.google.es).

- DRM: siglas en inglés de *digital rights management* (que en español se llama gestión de derechos digitales). DRM es una tecnología que permite a los creadores de contenidos digitales controlar cómo y quién accede a sus productos.

- FTP: siglas en inglés de *File Transer Protocol* (en español protocolo de transferencia de archivos). Es un protocolo de red empleado para copiar archivos de una computadora a otra a través de Internet.

- HASH:. Los hash o funciones "resumen" son algoritmos matemáticos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado (es decir, a partir de los datos de la entrada crea una cadena que solo puede volverse a crear con esos mismos datos). La palabra hash hace referencia a la función que se emplea, aunque por extensión también se utiliza para designar el resultado que se obtiene al aplicar la función. Por definición no pueden existir dos archivos distintos que tengan el mismo hash y además dos archivos que sólo se diferencien en un bit tendrán hashes totalmente distintos.

La función hash se utiliza para: identificar inequívocamente un archivo (es como el ADN de ese archivo), asegurar que no se ha modificado un archivo en una transmisión, hacer ilegible una contraseña o firmar digitalmente un documento.

- HTML: siglas en inglés de *Hypertext Markup Language* (lenguaje de marcado de hipertexto, en español), y es el lenguaje usado por los navegadores para interpretar y mostrar páginas de internet.

- HTTP y HTTPS: siglas en inglés de *HiperText Transfer Protocol* (en español protocolo de transferencia de hipertexto). Es un protocolo de red (un conjunto de reglas

a seguir) para publicar páginas de internet. HTTPS se usa para indicar que se está usando protección al transferir información.

- IM: siglas de mensajería instantánea (*instant messaging* en inglés) y es un servicio de comunicación de tiempo real entre dispositivos como computadoras, tabletas, teléfonos, etc.

- IMSI: acrónimo de *International Mobile Subscriber Identity* (Identidad Internacional del Abonado a un Móvil). Es un código de identificación único para cada dispositivo de telefonía móvil, integrado en la tarjeta SIM, que permite su identificación a través de las redes GSM y UMTS (3G). Este número de abonado conforme a la norma internacional ITU E.212, está compuesto por el MCC o código del País (3 dígitos), por ejemplo, *214*, que correspondería a España; por el MNC o Código de la red móvil (2 ó 3 dígitos), por ejemplo, *07*, que correspondería a la operadora MOVISTAR; y finalmente por el MSIN (número de 10 dígitos) que contiene la identificación de la estación móvil.

- IMEI: del inglés *International Mobile Equipment Identity* (Identidad Internacional de Equipo Móvil) es un código pre-grabado en los teléfonos móviles GSM/UMTS que identifica al aparato unívocamente a nivel mundial, y es transmitido por el aparato a la red al conectarse a ésta. Esto quiere decir, entre otras cosas, que la operadora que usemos no sólo conoce quién y desde dónde hace la llamada (SIM) si no también desde qué terminal telefónico la hizo. La empresa operadora puede usar el IMEI para verificar el estado del aparato mediante una base de datos denominada EIR (*Equipment Identity Register*). Se puede conocer tecleando "asterisco, almoadilla, 06, almohadilla".

- Ingeniería Social: es el proceso de manipular a usuarios legítimos para obtener información confidencial, con el objetivo de divulgar información, cometer fraude u obtener acceso a un sistema informático. Son técnicas basadas en engaños que se emplean para dirigir/controlar la conducta de una persona u obtener información sensible. El afectado es inducido a actuar de determinada forma (pulsar en determinados enlaces, introducir contraseñas, visitar páginas webs, etc.) convencido de que está haciendo lo correcto cuando realmente está siendo engañado por el ingeniero social. En el caso de las redes sociales, los atacantes disponen de una gran cantidad de información

tan sólo con ver el perfil de su víctima (sexo, fecha de nacimiento, aficiones, formación, carrera profesional, etc.) lo que favorece el despliegue y empleo de estas técnicas.

- Internet: en forma muy resumida, es una red de ordenadores o equipos informáticos que se comunican entre sí empleando un lenguaje común conocido como conjunto de protocolos TCP/IP. Contrario a la creencia popular, WWW no es un sinónimo de internet, es un servicio que es parte de internet.

- ISP o PSI: siglas en inglés de *Internet Service Provider* (en español: proveedor de servicios en Internet o PSI) término usado para referirse a empresas y organizaciones que proveen de conexión a internet (Access Provider) o servicios de internet (Service Provider) a sus clientes.

- Log: archivo que registra movimientos y actividades de un determinado programa (log file). Utilizado como mecanismo de control y estadística (por ejemplo, el log de un Web server permite conocer el perfil de los visitantes a un sitio Web).

- Login: proceso de seguridad que exige que un usuario se identifique con un nombre (user-ID) y una clave, para poder acceder a una computadora o a un recurso.

- MAC: la dirección MAC (no confundir con Mac de Apple) (siglas en inglés de *Media Access Control*; en español "control de acceso al medio") es un identificador de 48 bits que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física, y es única para cada dispositivo.

- Malware: es un término general que se le da a todo aquel software que tiene como propósito explícito infiltrarse o dañar a la computadora.

- Navegador (Browser/Web Browser): es un programa que permite ver páginas de internet. Específicamente traduce documentos escritos en HTML a contenido visible por personas.

- Nickname (Nick, sobrenombre o alias): nombre figurado que un usuario de internet utiliza, por ejemplo, para participar de un chat.

- Phishing: término empleado en el mundo de internet para referirse a un engaño o estafa diseñada para obtener información confidencial, como lo son números de tarjetas de crédito, claves de acceso, datos de cuentas bancarias u otros datos personales.

- Redes sociales: son plataformas Web compuestas por grupos de personas que forman una comunidad, y que a través de internet y de distintas herramientas interactivas, pueden relacionarse, comunicarse y compartir contenidos con otros miembros de esa misma comunidad o grupo, de un modo público o semipúblico, en función de las distintas posibilidades de asociación o acceso a la red y de los intereses, propiedades u objetivos comunes de dichos usuarios.

Desde un punto de vista general, la primera gran división a la hora de clasificar las redes sociales es en función de si se necesita o no un perfil para acceder a ella. En base a este criterio, las redes se clasificarían en:

a) Redes sociales directas: es necesaria la creación de un perfil por cada uno de los usuarios. Entre ellas cabría una segunda division atendiendo a :

- La finalidad: de ocio (Facebook, Tuenti, YouTube, Twitter), uso profesional (Facebook, Twitter, LinkedIn).
- El modo de funcionamiento: de contenidos (YouTube), basada en perfiles personales o profesionales (Facebook, LindekIn…), microblogging (Twitter)
- El grado de apertura: públicas (Facebook, Tuenti, YouTube…) o privadas (Yammer).
- El nivel de integración: vertical (acotado a un grupo de usuarios a los que les une una misma formación, interés o profesión (Dir&Ge) u horizontal (Youtube, Twitter, LindekIn).

b) Redes sociales indirectas: no es necesario la creación de un perfil. En este caso un usuario propone un tema y los demás pueden comentar o participar de esa aportación. En este apartado contaríamos con Foros y Blogs.

- Router: es un hardware que funciona a modo de semáforo para controlar el flujo de datos que se transmiten entre redes de ordenadores. Determina qué debe ir y a dónde. Es el encargado de guiar los paquetes de información que viajan por internet hacia su destino.

- Spyware: es un programa que se instala en el ordenador, usualmente con el propósito de recopilar y enviar información, que puede ser desde las costumbres de navegación en internet hasta números de tarjetas de crédito, claves de acceso, etc.

- SSL: son las siglas en inglés de *Secure Socket Layer*. Es un protocolo criptográfico empleado para realizar conexiones seguras entre un cliente y un servidor

- Troyano: es un malware destructivo que se disfraza de un programa benigno. Se diferencian de los virus en que los troyanos no se replican a sí mismos, aunque son igualmente peligrosos y destructivos.

- URI y URL: URI son las siglas en inglés de *Uniform Resource Identifier* y sirve para identificar recursos en Internet. URL son las siglas en inglés de *Uniform Resource Locator* y sirve para nombrar recursos en internet.

- Wi-Fi: es una marca registrada que también se usa como el término utilizado para nombrar la tecnología con la que se conectan diversos dispositivos electrónicos de forma inalámbrica.

PRIMERA PARTE

EL CIBERDELITO: ASPECTOS GENERALES Y CUESTIONES TÉCNICAS BÁSICAS.

CAPÍTULO PRIMERO

INTERNET Y LA CRIMINALIDAD.

1. ORIGEN Y EVOLUCIÓN DE INTERNET Y DE LOS DELITOS VINCULADOS.

No se puede avanzar en el estudio del ciberdelito sin hacer una somera referencia al origen histórico de internet y a sus características técnicas básicas. Es necesario conocer cuáles fueron las razones de su creación y los fines de su existencia, porque muchos de los problemas existentes al investigar un posible delito cometido haciendo uso de internet provienen precisamente de ese origen y de las características sobre las que está configurado[1].

Parece oportuno hacer una somera mención de las principales etapas por las que ha discurrido la implantación de internet y del modo en que ha ido apareciendo el nuevo elenco de conductas ilícitas vinculadas con la informática y la telemática.

La historia de internet es bastante compleja, por lo que para facilitar el estudio de su evolución y de las conductas delictivas vinculadas a la misma[2], distinguiré cuatro etapas que pueden caracterizarse por los intereses predominantes en cada una de ellas[3]:

---

[1] VAN EEKELEN, M.C.J.D & VRANKEND, H.P.E. *The Internet: Historical and Technical Background*, en"Cyber Safety: An Introduccion" (Leukfeldt & Stol, coord). Ed. Eleven International Publishing. La Haya, Holanda, 2012. págs 31 a 43.

[2] Para sistematizar la evolución de las conductas delictivas (o merecedoras de serlo) vinculadas con las Tecnologías de la información y comunicación, ver el estudio sobre la misma contenido en el *"Informe sobre la situación del crimen organizado en Europa"* realizado por el Consejo de Europa en 2004. Consejo de Europa: *"Organised crime in Europe: the threat of cybercrime. Situation report 2004"*, Francia, 2005. pags. 83 a 94.

[3] NOGALES FLORES, J.T. Tecnologías de Internet - T1: Naturaleza y evolución de Internet. https://aulaglobal2.uc3m.es/file.php/39339/html/doc/ti/ti-01.html 02/10/2012 0:24. Pág. 3. BARRY M. LEINER, VINTON G. CERF, DAVID D. CLARK, ROBERT E. KAHN, LEONARD KLEINROCK, DANIEL C. LYNCH, JON POSTEL, LAWRENCE G. ROBERTS, STEPHEN WOLFF Ilustraciones de KEVIN GRIFFIN Traducción: ALONSO ALVAREZ, LLORENÇ PAGÉS "Una breve historia de Internet (Primera Parte)", http://www.ati.es/DOCS/internet/histint/histint1.html 02/10/2012 0:35 ó http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet.

a) la denominada etapa militar, que se corresponde con la década de los años 70 del pasado siglo.
b) La denominada etapa académica: años 80 y primeros 90 del siglo XX.
c) La denominada etapa comercial: años 90 y posteriores.
d) La denominada etapa social: siglo XXI.

1.1 La denominada etapa militar.

Hablar del origen de internet es hablar de DARPA[4], acrónimo de la expresión en inglés *Defense Advanced Research Projects Agency*, Agencia del Departamento de Defensa de Estados Unidos, responsable del desarrollo de nuevas tecnologías para uso militar. Esta agencia, denominada originalmente como ARPA, fue fundada en 1958 como consecuencia tecnológica de la llamada Guerra Fría[5], y creó con carácter experimental una red informática llamada ARPANET[6] (Advanced Research Projects Agency Network), que estaba formada por los más prestigiosos centros de investigación académicos y militares del país, con el objetivo de compartir cualquier tipo de información necesaria disponible en cada uno de ellos.

Arpanet, antecesora de internet, se creó para conectar varios ordenadores de diferentes centros de investigación en una red[7]. Hasta ese momento todos los sistemas

---

[4] La *Advanced Research Projects Agency* (ARPA, Agencia de Proyectos de Investigación Avanzada) cambió su nombre a *Defense Advanced Research Projects Agency* (DARPA, Agencia de Proyectos de Investigación Avanzada para la Defensa) en 1971, es una agencia del Departamento de Defensa de los EE.UU, más tarde retomó su antigua denominación ARPA en 1993, para volver a DARPA en 1996. Me referiré siempre a ella con su nombre actual (DARPA).

[5] CURRAN JAMES. *Reinterpreting Internet history*. En "Handbook of Internet Crime". Ed. Willan Publishing, Devon, UK. Portland, Oregon USA. 2010. pág. 17. (Respuesta a la entonces URSS tras lanzar en 1957 el primer satélite espacial).

[6] http://www.computerhope.com/jargon/a/arpanet.htm. 7/10/2014 16.32. ARPANET o ARPANet , como precursor de internet, fue un proyecto conjunto entre Universidades, Centros de Investigación y DARPA, Departamento de Defensa de EE.UU. El servicio de la red Arpa demostró la utilidad de los protocolos TCP/IP ahora utilizados en internet.

[7] http://www.uned.es/dpto-eeyc/asignaturas/653060/Internet.doc 7/10/2014 a las 17.07. 5.1.- Definición de Internet. pág.7.
"Los principales objetivos de Arpanet fueron:
- Desarrollar una red que no se viese fuertemente debilitada en caso de que se perdieran partes físicas de la red, como podría ocurrir en caso de un conflicto nuclear.

de comunicación existentes eran sistemas punto a punto o extremo a extremo, que solo existía un canal de comunicación entre ambos extremos, y la supervivencia de esos sistemas de comunicaciones dependía de la existencia física del canal. La característica principal de Arpanet es que se desarrollaron e implantaron unos protocolos de comunicaciones que garantizaban la supervivencia de la comunicación en caso de que un enlace o canal fuera destruido en algún siniestro como pudiera ser un terremoto o un ataque nuclear[8]. Para ello, se prescindió de una red centralizada, y se descentralizaron todas las redes conteniendo rutas alternativas y redundantes entre los ordenadores conectados, de tal modo que cada ordenador formaba un nodo en la distribución de la red, ofrecía servicios a otros nodos, o usaba servicios de otros nodos dentro de la red. Nacieron así los protocolos distribuidos[9] que hacían posible que hubiera una comunicación entre dos extremos gracias a la existencia de múltiples caminos para que los mensajes alcanzasen su destino. Eran protocolos que permitían el intercambio de información con independencia de las conexiones físicas de los enlaces de comunicación. Además cada mensaje era dividido en paquetes y estos paquetes se distribuían y circulaban por los múltiples enlaces y rutas de comunicación. Era en el destino cuando se producía la reordenación de los paquetes entrantes y la confección del mensaje enviado.

En 1969 Arpanet contaba con cuatro ordenadores distribuidos entre distintas universidades del país. Dos años después, ya contaba con unos cuarenta ordenadores conectados[10], hasta el punto de que el rápido crecimiento de la red hizo que su sistema de comunicación de protocolos distribuidos quedara obsoleto, dando paso al Protocolo

---

- Que la red principal no debería ver afectadas sus prestaciones básicas con la incorporación de nuevos ordenadores dentro del sistema.
- Convertir a la red en un medio de comunicación independiente de la plataforma informática empleada lo cual aseguraría la compatibilidad ante cualquier circunstancia.".

[8] La creencia de que Arpanet se construyó para sobrevivir a ataques nucleares sigue siendo muy extendida. Sin embargo, hay muchos autores que no creen que éste fuera el motivo. Con independencia de ello, lo cierto es que Arpanet fue diseñada para sobrevivir a fallos en la red.

[9] Los protocolos distribuidos fueron el origen de los actuales protocolos de Internet *Protocolo NCP (Network Control Protocol), completado en 1972 y en uso hasta 1982, cuando fue sustituido por actuales TCP/IP (Transmission Control Protocol / Internet Protocol).* NOGALES FLORES, J.T. Tecnologías de Internet - T2: Protocolos de Internet e identificación de equipos. https://aulaglobal2.uc3m.es/file.php/39339/html/doc/ti/ti-02.html. 02/10/2013 a las 0.26, pag. 2.

[10] http://www.cad.com.mx/historia_del_internet.htm. 13/10/2014 a las 10.26.

TCP/IP, que se convirtió en el estándar de comunicaciones dentro de las redes informáticas[11].

En esta época inicial se empieza a producir la acumulación de datos de carácter personal de la ciudadanía por parte de los gobiernos, aun cuando no estaba masificado el uso de los ordenadores, y con ello comienzan las preocupaciones en torno al carácter reservado, la acumulación y el uso que podría hacerse de estos datos. Nace así el concepto de ***"privacy"*** y del derecho a la misma, que va más allá del tradicional concepto de intimidad y que regula la *acumulación en las bases de datos, de carácter informático o no, de información sobre los individuos y el uso que se hace de ella,* así como la capacidad de decisión de cada ciudadano respecto a qué datos referentes a su persona deben ser compartidos o públicos[12].

1.2 La denominada etapa académica.

A principios de los años 80 aparecen otras redes similares a Arpanet que pretenden dar cabida a investigadores no integrados en ella[13]. Se acentuó el carácter académico y de investigación ya que las funciones militares se desligaron de Arpanet y pasaron a MILNET (*Military Network o Military Net)*, una nueva red creada por los Estados Unidos que se integra en la *Defense Data Network* (1982).

La NSF *(National Science Foundation)* creó en el año 1984 su propia red informática con propósitos científicos y académicos llamada *NSFNET (National*

[11] Está formado por el Protocolo de Control de Transmisión (*Transmission Control Protocol*) y el Protocolo de Internet (*Internet Protocol*). El protocolo TCP divide en paquetes los mensajes generados en origen, asignándoles un número de secuencia y la dirección de destino, y los recompone en el destino, mientras que el protocolo IP se ocupa del direccionamiento de los paquetes (del transporte), que pueden recorrer el camino por rutas diversas, incluso con tecnologías diferentes.

[12] Ya en los años sesenta comenzaron las primeras discusiones en torno a esta cuestión, sobre todo en materia civil y administrativa, planteándose el debate, en los años siguientes, también en términos penales.

[13] NOGALES FLORES, J. T. Tecnologías de Internet - T1(…) Ob. cit. pág. 3 que comparten una disciplina científica (HEPNet, *High Energy Physics Network*, CSNET, *Computer Science Network*, 1981), una plataforma hardware (BITNET, *Because It's Time Network*, 1981, auspiciada por IBM, que no usa TCP/IP como tampoco su equivalente europea EARN, *European Academic and Research Network*, 1983), un sistema operativo (EUnet, *European UNIX Network*, 1982, JUNET, *Japan Unix Network*, 1984) y una localización geográfica (JANET, *Joint Academic Network*, 1984, del Reino Unido, con protocolos propios que mantendrá hasta 1991).

Science Foundation Network), que más tarde absorbió a Arpanet. Todas las redes de libre acceso se unieron también a *NSFNET*, formando el embrión de lo que hoy conocemos como *INTERNET*[14].

En 1985 internet ya era una tecnología establecida que se fue globalizando, cuando diversos países, sobre todo europeos, empiezaron a conectar sus redes académicas y de investigación a esta infraestructura (España lo hizo en 1990). Además, el incremento de los ordenadores personales trajo consigo el surgimiento de la piratería del software, dando lugar a las primeras infracciones contra la propiedad intelectual.

1.3 La denominada etapa comercial.

En 1990 ya deja de existir Arpanet como tal y se sientan las bases de la nueva etapa de internet de marcado carácter comercial que poco a poco va ganando terreno a la vertiente académica, debido a la aparición de aplicaciones revolucionarias[15] como WAIS, Gopher y aún más especialmente la *World Wide Web (WWW)* o telaraña mundial. En 1993 se produjo la primera versión del navegador *"Mosaic"*, que permitió acceder con mayor facilidad a la *WWW,* por lo que se abría la red a los legos[16]. A partir de entonces, internet comenzó a crecer más rápido que otros medios de comunicación,

---

[14] LADRÓN DE GUEVARA JIMÉNEZ, M. A. "Sistema operativo, búsqueda de la información: Internet/Intranet y correo electrónico". Ed. Tutor Formación, Logroño, 2014. pág. 71.

[15] http://www.uned.es/dpto-eeyc/asignaturas/653060/Internet.doc.8/10/2014 a las 13.49.
Wais (Wide Area Information Server): Servidor de información de área amplia que permite la búsqueda de material previamente indizado basándose en su contenido. Es un sistema diseñado para que el usuario pueda realizar consultas en una amplia red de bases de datos existentes en distintos servidores públicos. Ayuda a encontrar información deseada rastreando a través de los términos que hay dentro de los mismos documentos. Acceso a las bases de datos. Fue creado por Brewster Kahle y utiliza una arquitectura cliente/servidor.
Gopher: Sistema de acceso a internet con entorno gráfico. Creada en la Universidad de Minnesota, a finales de 1991.Esta herramienta facilita al usuario menús de opción con la intención de guiarle en la búsqueda de un determinado tema. Las búsquedas parten ordenadas según un criterio, de lo más general a lo más específico. Las opciones de búsqueda de documentos de Gopher las puede presentar mediante Archie, Wais, Telnet, FTP, WWW. Gopher permite examinar gran cantidad de información al ejecutar transferencias FTP, búsquedas Archie, etc.
WWW[15] o W3 o Web: Sistema creado para navegar por la red internet y acceder a miles de servidores donde encontrar información simplificada en su proceso de búsqueda y que proporciona información dotada de sonido, color, movimiento, etc. Contrario a la creencia popular, WWW no es un sinónimo de Internet, es un servicio que es parte de internet.

[16] LADRÓN DE GUEVARA JIMÉNEZ, M. A. "Sistema operativo, búsqueda de la información…", ob. cit. pág. 72.

convirtiéndose en lo que hoy todos conocemos: una red que dispone de multitud de servicios o aplicaciones que constituyen las herramientas de trabajo del usuario de internet[17].

El 24 de Octubre de 1995, el Consejo Federal de Redes (*Federal Networking Council*), responsable de la política de internet en Estados Unidos, aceptó unánimemente una resolución definiendo el término *Internet: "El FNC acuerda que la siguiente descripción refleja nuestra definición del término "Internet". Internet hace referencia a un sistema global de información que (1) está relacionado lógicamente por un único espacio de direcciones global basado en el protocolo de internet (IP) o en sus extensiones, (2) es capaz de soportar comunicaciones usando el conjunto de protocolos TCP/IP o sus extensiones u otros protocolos compatibles con IP, y (3) emplea, provee, o hace accesible, privada o públicamente, servicios de alto nivel en capas de comunicaciones y otras infraestructuras relacionadas aquí descritas"*[18].

La expansión de internet en la década de los noventa llevó aparejado el surgimiento de un nuevo método para difundir contenidos ilegales o dañosos, tales como pornografía infantil o discursos racistas o xenófobos. Serán precisamente las conductas vinculadas a la difusión de contenidos ilícitos las que más pueden

[17] Algunos de los servicios disponibles en internet además de la WEB son: el acceso remoto a otras máquinas *(SSH y telnet)*, transferencia de archivos *(FTP)*, correo electrónico *(SMTP)*, conversaciones en línea *(IMSN MESSENGER, ICQ, YIM, AOL, jabber)*, transmisión de archivos *(P2P, P2M, descarga directa)* etc. Vid. asimismo http://www.uned.es/dpto-eeyc/asignaturas/653060/Internet.doc. 07/10/2014, a las 14.51 horas, en la que se da cuenta entre otros de los siguientes servicios:
Telnet: Servicio de internet que permite el acceso a ordenadores mediante la emulación de terminal. Es una Herramienta que permite establecer sesiones de trabajo en un ordenador remoto desde el ordenador local, siempre que el usuario esté dado de alta en el sistema del ordenador remoto. Por lo tanto, permite trabajar interactivamente, ejecutar programas y utilizar recursos de otros ordenadores, que pueden estar situados a miles de kilómetros.
Transferencia de ficheros (FTP o *File Transfer Protocol*). Herramienta que se utiliza para conseguir información acerca de un tema concreto existente en los ficheros del ordenador de otro usuario. Es un protocolo que se utiliza para la transferencia de archivos en Internet a través de muchas plataformas. En la mayoría de los casos es necesaria una contraseña para acceder al archivo que contiene la información. En el caso que un fichero se encuentre liberado de contraseña se los denominan FTP anónimo.
Correo electrónico: Denominado en el argot "e-mail" (electronic mail), es el servicio más usado y uno de los más conocidos de internet, que permite enviar mensajes de cualquier índole (escritos, iconos) a otro/s usuario/s. Sus ventajas son: rapidez, economía y fiabilidad en cuanto a su recepción.
IRC (Internet Relay Chat) o Charla Interactiva en internet: Es un protocolo que permite mantener conversaciones en tiempo real con otro/s usuario/s de Internet. Ha evolucionado bastante, y ahora permite conversaciones de voz con otros usuarios, y también mantener videoconferencias.

[18] BARRY M. LEINER, VINTON G. CERF, DAVID D. CLARK, ROBERT E. KAHN, LEONARD KLEINROCK, DANIEL C. LYNCH, JON POSTEL, LAWRENCE G. ROBERTS, STEPHEN WOLFF Ilustraciones de KEVIN GRIFFIN Traducción: ALONSO ALVAREZ, LLORENÇ PAGÉS "Una breve historia de Internet (Segunda Parte)", http://www.ati.es/DOCS/internet/histint/histint2.html 02/10/2012 0:36, pág. 6.

aprovecharse de la enorme implantación que tiene la red a nivel mundial, así como de sus características técnicas que dificultan su descubrimiento, persecución y prueba.

1.4. La denominada etapa social.

Paulatinamente se han ido incorporando a internet nuevos protocolos y formas de uso que fomentan la comunicación entre usuarios particulares o grupos de usuarios y la participación en actividades cooperativas. Lo que en general se ha llegado a denominar Web 2.0, con servicios como los diarios personales (blogs), las redes sociales, las enciclopedias colaborativas, el etiquetado social de recursos, etc., que han hecho de internet un medio activo en el que el usuario particular aporta y comparte información y ya no se limita a recibirla[19]. La facilidad en el acceso y en la búsqueda de información contenida en redes y sistemas informáticos, combinada con las prácticamente ilimitadas posibilidades para su intercambio y difusión ha llevado a un crecimiento explosivo en la cantidad de información accesible siendo significativa la progresiva generalización del uso del correo electrónico y el acceso a través de internet a numerosos sitios o páginas web de distintas partes del mundo.

En este período también se consolida la dependencia que los gobiernos y organismos internacionales tienen de los sistemas informáticos, tanto para su buen funcionamiento como para el almacenamiento de datos importantes y/o secretos *y* ello los pondrá en el punto de mira para la comisión de delitos que atenten contra la seguridad del Estado o para la comisión de ataques terroristas a través de la red.

Internet ha generado nuevas oportunidades de enriquecimiento ilícito en forma de estafas y fraudes en las que no sólo intervienen delincuentes individuales sino grupos criminales. Por otro lado, los beneficios obtenidos por las organizaciones criminales les capacitan para acceder a casi cualquier recurso tecnológico, lo cual les sitúa en una posición de ventaja para explotar nuevas oportunidades de negocio y anticiparse a la actuación de las agencias de seguridad, normalmente peor dotadas en ese sentido. Siendo Europa un continente con gran acceso y disponibilidad de internet por la

[19] NOGALES FLORES, J.T. Tecnologías de Internet - T1(…). ob. cit. pág. 4.

población, el desarrollo de actividades ilegales y fraudes a través de esta herramienta también se multiplica[20]. En el primer decenio del siglo XXI han predominado nuevos y sofisticados métodos para delinquir[21], y el uso de tecnologías que dificultan la investigación penal[22].

En definitiva, internet ha cambiado notablemente en su corta existencia, creciendo hasta convertirse en una infraestructura informática ampliamente extendida con capacidad para interconectar a todo el planeta[23], ignorando fronteras políticas y superando barreras geográficas, lingüísticas, culturales o religiosas, sentando las bases de lo que se conoce como *Sociedad de la Información*[24].

Consecuentemente, los delincuentes también han hecho uso de las oportunidades que ofrece internet y los delitos cometidos en la red o con ocasión del uso de nuevas tecnologías están en alza dada la rapidez con la que éstas evolucionan[25]. El interrogante ante tal evolución es cómo hacer frente a esta nueva actividad criminal, lo que supone un auténtico desafío en el que están implicados todos los poderes del Estado[26].

---

[20] GIMÉNEZ-SALINAS FRAMIS, A. La Lucha contra el crimen organizado en la Unión Europea. Documentos de Seguridad y Defensa 48. Centro Superior de Estudios de La Defensa Nacional. Ed. Ministerio de Defensa, Madrid 2012. pág. 25.

[21] Tales como la "pesca de datos" o "phishing" y los ataques con redes zombi o "botnets".

[22] Tales como las comunicaciones con transmisión de voz sobre Protocolo de Internet (VoIP) y la informática en nube ("cloud computing"). XII Congreso de Naciones Unidas sobre Prevención del delito y Justicia Penal. Tema 8 del programa "Novedades recientes en el uso de la ciencia y la tecnología por los delincuentes y por las autoridades competentes en la lucha contra la delincuencia, incluido el delito cibernético".

[23] En 2015 se superó la barrera de 3000 millones de internautadas de la población mundial. En "La Sociedad de la Información en España 2015_siE[15". Fundación Telefónica. Ed. Ariel, Barcelona, 2016. pág. 33 http://www.fundacion.telefonica.com/es/arte_cultura/publicaciones/detalle/258.

[24] NOGALES FLORES, J.T. Tecnologías de Internet - T1(…). ob. cit. pág. 2.

[25]ALVAREZ MONTOYA, W. 6.1. INTRODUCCIÓN. Breve Historia de Internet. En http://www.unalmed.edu.co/~incominf/W8070[6-1].htm. 8/10/2014 a las 16.27.

[26] Esos progresos han tenido también su reflejo en la delincuencia y criminalidad. Han aparecido nuevos tipos de delitos, así como nuevas modalidades y peculiaridades en la comisión de los clásicos delitos. Más aún, las consecuencias de la conducta criminal pueden ser de mayor entidad y trascendencia puesto que no están restringidas por limitaciones geográficas o fronteras nacionales. La propagación mundial de virus informáticos, como por ejemplo el virus "I love you" por un estudiante desde Las Filipinas afectando a miles de equipos y sistemas informáticos, proporcionó una prueba de esta realidad. Desde muchos ámbitos doctrinales, nacionales y extranjeros, se han propugnado como medidas más eficaces y adecuadas para hacer frente a los retos de la delincuencia informática las medidas técnicas de autoprotección, sin embargo la experiencia criminológica de los últimos años ha demostrado que las

2. FACTORES DE INTERNET QUE FAVORECEN LA COMISIÓN DE LOS DELITOS.

2.1 Nociones básicas de internet.

Cómo ya se adelantó supra, es preciso conocer las reglas técnicas básicas sobre las que se configura internet, pues su conocimiento facilita la comprensión del ciberdelito y del proceso de investigación que podrá llevar a determinar el origen de la acción delictiva, para a su vez poner de manifiesto en qué medida dichas características influyen y favorece la comisión de determinados delitos.

2.1.A) Características técnicas.

- Conmutación de paquetes[27]: en internet, la información, el mensaje a trasmitir (texto, voz, datos, imágenes, video) se divide en trozos llamados paquetes, que son enviados de forma independiente a su destino, y pueden seguir diversas y diferentes rutas para alcanzarlo. Una vez en el destino, los diferentes paquetes se unen para formar el mensaje. En este sistema de conmutación de paquetes, a diferencia de los sistemas de comunicación tradicional (como por ejemplo telefónico) no hay una sola conexión entre el que envía el mensaje y quién lo recibe, sino que las conexiones de la red pueden ser compartidas para transportar paquetes correspondientes a múltiples mensajes de diferentes usuarios.

- Addressing and routing: en el sistema de conmutación de paquetes no hay una noción de una conexión fija entre el origen y el destino. Cada paquete además contiene la dirección del receptor. La red usa esta dirección para enviar el paquete a través de alguna ruta desde el emisor hasta el receptor. Este enrutamiento está hecho por unos dispositivos denominados "enrutadores" o "*routers*", que no son sino unos equipos

mismas, siendo necesarias, son insuficientes, superadas de continuo por los delincuentes, y de un alto costo para los sujetos pasivos afectados.

[27] Esta técnica es llamada *packet switching*. VAN EEKELEN, M.C.J.D & VRANKEND, H.P.E. The Internet: Historical (…) ob. cit. pág. 32.

especiales en la red que envían los paquetes a la dirección correcta desde el origen a su destino. Los *routers* intentan evitar la congestión de la red, y para ello los paquetes pueden ser enviados a través de caminos diferentes hacia el destino. Los paquetes pueden seguir diferentes rutas y llegar al destino en diferente orden en el que fueron enviados. Además los paquetes se pueden perder o corromper durante la trasmisión, por ejemplo debido a interferencia o sobrecarga de la red. En ese caso se vuelve a enviar el paquete, ya que internet ha sido diseñado para tratar estos problemas y que los usuarios finales no tengan que preocuparse, pues proporciona una comunicación segura a los usuarios finales incluso si se rompe la infraestructura de red subyacente o fuera inestable o no fiable.

- Protocolos de Comunicación (*Protocol Layers)*: en general, un protocolo de comunicación define qué mensaje puede ser enviado y en qué orden entre dos partes; es decir, simplemente describe el formato de los mensajes y las reglas que hay que seguir para transmitirlos de un sistema a otro. El protocolo de comunicación usado en internet es algo más complejo. Las diferentes aplicaciones que existen, tales como *World Wide Web*, *Email* o *File Transfer*, requieren diferentes protocolos. Para tratar con esta complejidad los protocolos de internet se dividen en una serie de capas[28] (*Layers),* de forma que cada capa proporciona una función básica que puede ser usada por la siguiente capa.

Inicialmente Arpanet tenía dos capas, pero esta arquitectura era demasiado restrictiva con los diferentes tipos de ordenadores de los usuarios. Además la red estaba formada por diversos medios de transmisión como ondas de radio trasmitidas por satélite, señales eléctricas a través de todo tipo de cables y señales de luz a través de fibra de cristal. Mediante la división de la funciones de comunicación sobre capas y describiéndose claramente las *interfaces* entre las capas, fue posible conectar la red.

[28] *Stack of layers.* VAN EEKELEN, M.C.J.D & VRANKEND, H.P.E. *The Internet: Historical* (…) ob. cit. pág. 33. Este sistema de capas es parecido en algunos aspectos al correo postal, en el cual el remitente deja la carta en el buzón, el servicio de correos la recoge y el cartero la entrega al destinatario. El protocolo que interesa al remitente y al receptor es que se mande la carta y para hacer eso ellos usan el servicio que ofrece la compañía postal. El remitente y destinatario no tienen que preocuparse en el modo en el que la compañía postal envía la carta. Por lo tanto en este ejemplo hay dos capas: la capa del remitente y destinatario y la capa de la compañía postal.

Además cuando se introduce una nueva aplicación o un nuevo medio de comunicación, lo único relevante es que la capa tiene que ser adaptada o extendida[29].

- Número de puerto, dirección IP, dirección MAC: a cada paquete se le añade una cabecera en cada una de las capas. En la capa aplicación se le añade lo que se denomina número de puerto (*port number)*. El número de puerto indica la aplicación a la que el paquete corresponde, por ejemplo, el correo electrónico (SMTP) usa el puerto número 25, el navegador web (HTTP protocol) usa el puerto 80, etc..

En la capa de red la cabecera que se añade contiene la dirección IP, usada por los routers para enviar el paquete a través de la red. La cabecera en la capa de enlace de datos contiene la dirección *Media Acces Code (MAC),* la cual es una única dirección que identifica al dispositivo en la capa de enlace.

[29] Ya se ha hecho referencia a que en 1983 ARPANET introdujo el llamado protocolo TCP/IP y el término internet comenzó a usarse. Este protocolo de comunicación fue dividido en cinco capas:

- Capa de aplicación (*Application layer*).
- Capa de Transporte (*Transport layer*)
- Capa de red (*Network layer*).
- Capa de enlace de datos (*datalink layer*).
- Capa física *(Physical layer)*.

El Término TCP/IP proviene de dos de los protocolos más importantes, el *Transmission Control Protocol* (TCP) en la capa de transporte y el *Internet Protocol* (IP) en la capa de red.

La Capa de Aplicación utiliza los protocolos de las capas inferiores que gestionan el transporte real. La capa de aplicación contiene sus propios protocolos como *Simple Mail Transfer Protocol (*SMTP) para emails, *File Transfer Protocol* (FTP) para transferencia de archivos, y *Hyper Text Transfer Protocol* (HTTP) para la World Wide Web. Cada protocolo define qué información es intercambiada entre el emisor y receptor para una particular aplicación.

La Capa de Transporte contiene dos protocolos: *Transmission Control Protocol* (TCP) y *User Datagram Protocol* (UDP). TCP es usado para asegurar que cada paquete es recibido correctamente al destino y proporciona una comunicación segura, lo que requiere de algún acuse de recibo. Por ejemplo, el receptor envía un acuse de recibo a cada paquete del remitente, para indicar que le llegó correctamente. Si un remitente no recibe un acuse de recibo, enviará el paquete de nuevo después de un cierto tiempo. Aunque TCP es fiable, no es rápido. UDP, es una rápida alternativa a TCP pero es menos seguro. El acuse de recibo de la recepción o retransmisión de los paquetes no está incluido en UDP. Para aplicaciones donde la seguridad de recibir es realmente importante como el envío de archivos, TCP es el protocolo preferido. Pero para aplicaciones donde ese acuse de recibo de la recepción es menos importante, como escuchar un audio en tiempo real, el protocolo UDP es preferido.

La Capa de Red contiene un protocolo: *Internet protocol* (IP) que une las diferentes redes y las rutas de los paquetes a través de estas redes basadas en la direcciones IP.

La Capa de Enlace de Datos contiene una gran variedad de protocolos afines a la red física. La capa de enlace de datos es usada para mover paquetes entre dos ordenadores principales conectados al mismo enlace de comunicación. El protocolo de la capa de enlace más conocido es *Ethernet protocol,* usado en la red local.

La capa física es la capa donde los bits son usados como señales físicas (eléctricas, electromagnéticas u ópticas) en un medio físico. Los protocolos en esta capa están relacionados con las tecnologías de transmisión (cable, fibra óptica, ondas de radio, microondas, etc.) de la red, en el cual los bits de información son transformados para poder ser enviados sobre un enlace físico.

- Gestor de las direcciones IP y nombres de dominio: una única dirección IP es asignada a cada dispositivo que se conecta a internet a través del interfaz de red que usa el protocolo IP para dirigir los paquetes a los dispositivos[30].

Los usuarios que deseen acceder a internet necesitan obtener una dirección IP del *Internet Service Provider*[31] (*proveedor de acceso o servicio de internet)*. Cuando se accede a internet, el Servidor (ISP), asigna un número denominado IP (Internet Protocol), que identifica en todo momento al usuario mientras permanezca en ella. Haciendo un símil, al entrar en la red por una puerta o ISP, el administrador de esa puerta nos entregará un ticket numerado (IP), que devolveremos al salir. En ese momento, en toda la red seremos los únicos que tendremos esa numeración. A cuantos lugares accedamos de la red, nuestro ticket (IP), dejará una marca. De esta forma, para saber quién ha accedido a un punto concreto de la red en un momento determinado, debemos consultar el ticket (IP), averiguar a que puerta (ISP) pertenece y a que usuario fue asignado por el administrador de esa puerta en ese momento determinado. Conocida una IP, la identificación del ISP a que corresponde es de dominio público a través de unas bases de datos que existen en internet (RIPE, WHOISdb, etc.)[32], en la cual aparecen los datos y un lugar físico de ubicación de los proveedores de Servicios que los asignan. Estos proveedores de internet, ISP debido al gran número de usuarios que gestionan, guardan por un espacio de tiempo los registros de la conexión, datos que identifican a un usuario que realiza la conexión desde una línea telefónica concreta, por lo cual se hace necesario actuar con gran rapidez. No obstante, puede darse que las IP

[30] Cuando se desarrolló el protocolo IP, se pensó que el número de direcciones IP era más que suficiente, pero en la actualidad, con la expansión, crecimiento y desarrollo de nuevos servicios y dispositivos conectados a Internet, existe carencia de direcciones IP. Para solucionar este problema se ha desarrollado un nuevo protocolo IP, denominado IP versión 6, que soluciona definitivamente el problema de la falta de direcciones. Las direcciones IP inicialmente tenían una longitud de 32 bits y por tanto había 2 elevado a 32 (casi 4.3 billones de diferentes direcciones IP. La estructura numérica es llamada IPv4 (versión 4). En 2011, la última dirección IPv4 fue emitida por ICANN. El sucesor de la versión 4 del IP es la versión 6, la IPv6 con una longitud de 128 bits, por lo que hay 2 elevado al 128 (3.4¨10 elevado a 38) de diferentes direcciones IP, con lo cual excede del número de átomos sobre la faz de la tierra. NOGALES FLORES, J.T. Tecnologías de Internet - T2(…) ob. cit. pág. 3.

[31] ISP son las siglas en inglés de "*Internet Service Provider*" -en español: proveedor de servicios en Internet o PSI-, que es un término usado para referirse a empresas y organizaciones que proveen de conexión a Internet (Access Provider) o servicios de Internet (Service Provider) a sus clientes.

[32] https://www.ripe.net 21/01/17 a las 18.50.
https://www.whois.net 21/01/17 a las 18.55.

objeto de la investigación pudieran tratarse de un Proxy Cache[33], o igualmente se puede dar el caso de que algunos usuarios oculten su IP a través de diferentes programas existentes en la red conocidos como navegación anónima[34].

Los ISP obtienen las direcciones IP de *Internet Corporation for Assigned Names and Numbers* (ICANN)[35] un organismo independiente que suministra las IP mundialmente[36] y también los nombres de dominio (DNS, *Domain Name System*) [37].

[33] Es por lo que de forma breve se explicará lo que es un Proxy Cache. En informática, se utilizan sistemas caché, que almacenan temporalmente la información utilizada, porque está comprobado que esa misma información suele volver a necesitarse. Este truco tiene cierto sentido cuando el sistema de almacenamiento temporal es mucho más ágil (rápido de consultar) que la fuente original que contenía la información. Muchas páginas son consultadas repetidamente al cabo del día, el proveedor de conexión puede instalar un sistema que actúe como memoria temporal intermedia para guardar una copia de las páginas que van visitando los usuarios. Así, cuando otro internauta (o el mismo) quiera volver a consultar esa página, el proveedor de internet ya no necesita solicitar al servidor que la aloja en otro ordenador remoto: puede pasarle al usuario los datos (una "copia) que están almacenados en alguno de sus propios ordenadores. Este sistema se le suele denominar PROXY-CACHÉ o PROXY-TRANSPARENTE.

[34] Si se utiliza uno de estos programas, él mismo nos buscará conexiones de proxys o bien conexiones utilizando proveedores de Internet que se encuentran en el extranjero.

[35] http://www.icann.org/ 23/02/2014 18.18.

[36] ICANN asigna bloques de números IP a los ISP. Por tanto cada ISP tiene un suministro de IP que proporciona a sus clientes. Esto significa que no todas las IP son realmente usadas. Hay un gran número de ISP que han acoplado sus redes a otras ISP. Parte de la infraestructura física de las redes son propiedad de muchas otras organizaciones, algunas de las cuales operan en internet. Estas compañías ofrecen su infraestructura de redes a otras ISP. Por lo tanto, las ISP pueden que no sean propietarias de la infraestructura de red física, solo operan en ella.

[37] Un nombre de dominio es una cadena de caracteres legible que se corresponde a una dirección IP. El cerebro humano puede recordar mucho mejor el significado de un nombre que una secuencia arbitraria de números. Por ello, el sistema de nombres de dominio DNS es un sistema de base de datos distribuido en todo el mundo que almacena las relaciones entre la dirección IP y los nombres de dominio, como si de un catálogo de números de teléfonos se tratara. El sistema DNS está compuesto por los nombres de dominio de los servidores que se organizan en una estructura jerárquica. Por ejemplo, cuando un usuario quiere acceder a google.es, se obtiene la dirección IP correspondiente al nombre de dominio y la web de google puede ser contactada.
Es obvio que el nombre de dominio www.google.com corresponde a google. La extensión ".com", indica el *Top Level domain* (TLD). Internet está dividido en grandes dominios o dominios de nivel superior: La mayoría de los países tiene su TLD, así en España el TLD es (.es), en Francia (.fr), USA (.us). También hay TLDs en otras estructuras organizativas, por ejemplo *.com* para empresas, *.edu* para instituciones educativas, *.org* para organizaciones. ICANN ha proporcionado una largo número de otras TLDs como . *info* o *.biz*.
NOGALES FLORES, J. T. Tecnologías de Internet - T2(…) ob. cit. pág. 5. Los nombres de dominio son importantes en el marketing, y con frecuencia el nombre de dominio se corresponde con la marca o nombre de la organización. Algunos pequeños países ganan dinero vendiendo el nombre de dominio. Tal es el caso de Tuvalu, una pequeña isla localizada en el Océano Pacífico ganó millones de dólares por el alquiler de sus *.tv* TLD.

2.1.B) Componentes técnicos.

Internet tiene una estructura distribuida, no jerárquica, consistente en una red troncal de servidores (*hosts*) u ordenadores principales, a los que se conectan las redes de acceso y las redes de área local (LANs). Cada uno de los componentes de internet tiene su propio papel: *routers*, redes de acceso, redes de área local y servidores u ordenadores principales.

- Routers: los *routers* se encargan de interconectar los servidores y las diferentes redes pues son dispositivos especializados que enrutan los paquetes a través de internet, sobre la base de la dirección IP del receptor. El enrutamiento se realiza con algoritmos complejos. No sólo el camino más corto o más rápido entre el origen y el destino es considerado durante el enrutamiento, sino también el costo involucrado, basado en acuerdos entre los ISP y las empresas de la red.

- Redes de Acceso (*Access networks*): inicialmente los usuarios privados y las pequeñas compañías estaban físicamente conectados a internet a través de la red telefónica básica. Un dispositivo especial, llamado modulador/demodulador (módem), transformaba la señal analógica de la línea telefónica en una señal digital para la entrada/salida en el ordenador. El uso de la red telefónica analógica implicaba que los costes cargados estaban basados en la cantidad de tiempo que la conexión utilizaba en realidad, similar a las llamadas telefónicas tradicionales. Hoy en día, las conexiones a internet por la red telefónica, en su mayoría utilizan la línea de abonado digital asimétrica *Asymmetric Digital Subcriber Line* (ADSL), que ofrece una conexión permanente y de gran ancho de banda en contra de los costes fijos. Las redes de cable, inicialmente utilizadas exclusivamente para las señales de televisión de difusión, también se utilizan para conectarse a internet. Estas redes de cable que inicialmente consistían en gran parte en hilos de cobre, ahora están siendo reemplazadas por la fibra óptica que ofrece un gran ancho de banda.

El desarrollo tecnológico experimentado en los últimos años que aprovecha la propagación de señales electromagnéticas a través del espacio radioeléctrico ha permitido utilizar como Red de Acceso a internet los diferentes servicios de telecomunicaciones inalámbricas. Las distintas tecnologías (GSM, 3G, WiFi, WiMax,

LMDS, etc.) permiten proporcionar acceso a internet a los más variopintos dispositivos (portátiles, teléfonos móviles, tabletas, videoconsolas portátiles, etc.).

- Redes de Área Local (*Local Area Networks)*: Los ordenadores suelen estar conectados en red formando lo que se conoce como red de área local *local area network* (LAN). Las LAN pueden interconectarse a internet por medio de un router o incluso por medio de un módem y un router. El módem se encarga de la conexión física y la trasformación de las señales físicas, mientras que el router gestiona el tráfico de datos entre la LAN e internet. También puede jugar un papel importante en la seguridad, por ejemplo, puede implementar un servidor de seguridad para filtrar el tráfico no deseado. En los últimos años la conexión wireless (inalámbrica) se ha hecho muy popular. Una red inalámbrica puede ser parte de una LAN y los dispositivos móviles como portátiles pueden fácilmente conectarse. También hay muchas redes inalámbricas que permiten el acceso público.

- Servidores o *Hosts*: Los *Hosts* (ordenador principal) son los sistemas informáticos que forman los nodos de internet. Estos hosts pueden ser equipos informáticos de usuarios individuales, o pueden también ser servidores conectados a internet de empresas.

Muchas aplicaciones en internet son distribuidas, dentro del modelo de relación cliente-servidor. Un cliente es un ordenador que usa el servicio ofrecido por los servidores. Un servidor es un ordenador que ofrece servicio al cliente. Ejemplo de servidores son los servidores de páginas Web, o los servidores de correo electrónico, o los servidores de ficheros, que juegan todos ellos un papel esencial en internet.

2.1.C) Aplicaciones y servicios.

Internet es la infraestructura de red, la red de redes, que puede ser usada por todo tipo de servicios y aplicaciones. En esta sección se describirá *The World Wide Web* que es la aplicación más popular de internet, las restricciones de acceso a partes de internet y otros servicios ofrecidos por internet.

- World Wide Web: desde mediados de los 90 la aplicación más popular de internet es la World Wide Web (WWW). La organización W3C (World Wide Web Consortium) ha guiado el desarrollo de los estándares www. Los ISPs operan muchos de los servicios de internet para almacenar y administrar páginas web, buzones de correo y nombres de dominio. Usando el protocolo http, se accede a los servicios de world wide web, utilizando un programa informático específico llamado navegador (internet explorer, safari, firebox, chrome, mozzila). Como el acceso a internet es muy común a través de un navegador, se suele identificar la World Wide Web con internet. Pero internet es más que eso, es la infraestructura que conecta todos los dispositivos y WWW es una de sus aplicaciones.

- Dominios de internet blindados: la idea inicial de internet, donde los ordenadores cliente podían acceder a los servicios sin restricciones, ha sido redefinida años más tarde. Hoy muchos servicios y servidores son accesibles sólo para un grupo limitado de usuarios. El blindaje de servicios y servidores es implementado por medidas a nivel de la red y a nivel de servidor de manera que se produce una separación entre redes dando lugar a los conceptos de intranet y extranet.

Una intranet es una red privada de ordenadores en la que se implementan los mismos protocolos utilizados en internet. Las intranets son típicamente redes internas dentro de organizaciones que pueden estar o no conectadas a internet. En el caso de estar conectadas a internet, la interconexión se realiza de manera segura a través de unos dispositivos de protección denominados cortafuegos. Los cortafuegos aseguran que se pueda acceder a los servicios de internet desde la intranet pero sin embargo prohíben que desde internet se pueda acceder a los servicios de la intranet. Una extranet puede ser considerada como una extensión de una intranet. Los servicios de la extranet pueden ser accedidos desde la intranet, utilizando internet como medio de transporte, lo que se consigue con técnicas de control como por ejemplo usando el nombre de usuario y la contraseña, o utilizando mecanismos que implementan lo que se conoce como red privada virtual *virtual private network* (VPN).

- Navegadores (Web Browsers): Los navegadores web son usados para recuperar y presentar información desde el www usando el protocolo http en la capa de aplicación. Hypertext Tranfer Protocol Secure (HTTPS) es una versión de seguridad

mejorada de la versión http, que proporciona el cifrado de datos y autenticación de servidor y cliente.

El contenido y formato de una página web es descrito utilizando un lenguaje de marcado denominado Hypertext Markup Languague (HTML). El código HTML es interpretado por el navegador representando en pantalla la página web tal como ha sido diseñada. Las páginas web pueden contener texto, imágenes, sonido y video. El navegador tiene una estructura modular y puede ser extendido con plug-ins para mejorar y representar contenido de otras aplicaciones, como por ejemplo las aplicaciones de animación tipo flash. De este modo, una página web puede contener elementos interactivos[38].

- Cookies: una cookie es un paquete de datos que un navegador web almacena de forma automática en el ordenador de un usuario cuando este visita una página web. La cookie es enviada desde el servidor al visitante de la página web. Posteriormente, cada vez que el usuario visite esa misma página web o alguna otra del mismo dominio, la cookie será leída por el navegador web, sin ser modificada, y devuelta al servidor web. Por tanto, una cookie son sólo datos que se almacenan en el ordenador del usuario[39].

- La Internet Profunda o "Deep Web": más allá de la superficie de la web, existe una web incluso más amplia, llamada "*Deep Web"* (Web profunda), a la cual es mucho más difícil de acceder. Esta dificultad no es debida a que estas páginas estén protegidas por cortafuegos o sean sólo accesibles en la intranet[40]. La Deep Web se refiere a información a la cual se accede a través de la web pero que está almacenada en bases de

[38] La interactividad en una página web puede ser proporcionada por lenguajes de programación como Java applets o JavaScript. JavaScript es un lenguaje compatible con la mayoría de los navegadores. El código javascript es descargado del servidor y ejecutado por el navegador web, lo que permite interactuar con páginas web pero también descargar y ejecutar códigos javascript maliciosos sin conocimiento.

[39] Pero como el almacenamiento se realiza por orden del servidor web, siempre ha existido el miedo de que se pudiera hacer algo malicioso. Sin embargo, las cookies no son software ni tampoco fragmentos de código sino que son simplemente datos. Por tanto, en principio las cookies no pueden transmitir y ejecutar virus, ni instalar malware como troyanos o programas de espionaje, pero sí que pueden ser utilizadas para realizar un seguimiento de la actividad de un usuario en la Web. Los navegadores web permiten a los usuarios decidir si aceptan las cookies o no pero muchas veces el rechazar la cookie hace que no se pueda acceder a la página web.

[40] ÉCIJA BERNAL, A. "Ciberespacio, darkweb y ciberpolicía". Diario La Ley nº 2, Sección Ciberderecho, 4 de Enero de 2017. pág. 2.

datos a las que se pueden entrar produciendo páginas web. Los catálogos de productos son un ejemplo de estas páginas web. La estructura y tamaño de la Deep Web es difícil de medir[41].

2.2 Internet y el cambio en la concepción tradicional del delito.

Una vez vistas las características técnicas básicas que presenta internet, procede tratar ahora en qué medida esas características son particularmente relevantes a la hora de facilitar la comisión del delito[42], para analizar a continuación los problemas y retos que plantea la aparición de los nuevos tipos penales de la sociedad de la información[43].

Tal como ha quedado dicho, internet es una red mundial con conexiones instantáneas y con una estructura descentralizada que se basa en la representación digital de la información y que permite las conexiones en tiempo real entre las personas independientemente de su ubicación. Ello ofrece oportunidades especiales para cometer delitos, pues el tiempo, la distancia y las fronteras nacionales son mucho menos importantes que en los delitos tradicionales[44]. Pues bien, todas estas características relacionadas entre sí representan las peculiaridades que favorecen la comisión de ciertos delitos lo que dificulta al mismo tiempo su investigación y persecución judicial, a saber[45]:

---

[41] VAN EEKELEN, M.C.J.D & VRANKEND, H.P.E. *The Internet: Historical* (…) Ob. cit. pág. 43. Para entrar en la Deep web hay que instalar un navegador, conocido como red TOR. Esta internet profunda es usada por los delincuentes para la venta de armas, de drogas, pornografía infantil etc. Presenta como característica que es muy difícil investigar quién está detrás de esas páginas. Una vez dentro de la Deep Web te conviertes en un nodo pero se olvida el anterior, por lo que es difícil seguir el rastro.

[42] KOOPS, BERT-JAAP. *The internet and its opportunities for cybercrime. "*Transnational Criminology Manual".(M. Herzog-Evan, coord.). Ed. Wolf Legal Publishers, Nijmegen, 2010, págs. 735-754. http://arno.uvt.nl/show.cgi?fid=113411.

[43] DÍAZ GÓMEZ, A. "El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest*"*. Revista electrónica del Departamento de Derecho de la Universidad de La Rioja, REDUR 8, diciembre 2010, pág. 173.

[44] TEJADA DE LA FUENTE, E. "Problemas generales en la investigación de la criminalidad informática". Ponencia presentada en el curso Menores e Internet año. 2012.www. cej.mjusticia.es. págs. 9 a 13.

[45] KOOPS, BERT-JAAP. *The internet and its opportunities* (…) ob.cit. págs. 735 a 754.

1. El desarrollo de internet ha tenido su reflejo en la delincuencia y la criminalidad, pues han aparecido nuevos tipos delictivos, así como nuevas modalidades en la comisión de delitos tradicionales. Actualmente lo informático se constituye no sólo en un medio sino incluso en un objeto potencial para la realización de ilícitos estrictamente telemáticos o cibernéticos[46].

2. Internet es una red mundial que presenta un alcance global a la que se puede acceder desde cualquier parte del mundo prácticamente al instante. Ello permite que los potenciales delincuentes puedan actuar desde cualquier lugar del mundo, buscar a las víctimas más vulnerables en cualquier lugar y efectuar los ataques también en y desde cualquier lugar, evitando la persecución gracias a la deslocalización que ofrecen este tipo de actividades cibernéticas. Internet y su desarrollo global no sólo ha acrecentado su significación criminológica, sino que ha dificultado en mayor grado la posibilidad de acreditación del hecho punible, de las personas responsables, e incluso del equipo origen de la acción ilícita.

3. Este alcance global conduce a la desterritorialización, lo que implica que el fenómeno de la ciberdelincuencia sea casi por definición, internacional. Ello conlleva dificultad en la persecución de los delitos con los consiguientes desafíos legales de la cooperación internacional para perseguir un ilícito de estas características. Piénsese, por ejemplo, que un sujeto puede cometer un delito contra otro situado a miles de kilómetros del primero, mientas que la información está en otro lugar diferente de éstos. Se ha acrecentado la característica transnacional o transfronteriza de estos delitos, con los consiguientes problemas competenciales entre jurisdicciones de distintos Estados, la disparidad de sus normativas penales en la sanción de una misma conducta, o incluso su consideración o no como delito[47] y la existencia de los

[46] ROVIRA DEL CANTO, E: "Las nuevas pruebas telemática y digitales. Especialidad de la prueba en delitos cometidos por internet". Jornadas sobre la prueba en el Proceso Penal. Estudios Jurídicos, Ministerio Fiscal, Vol. I-2003. C.E.J.A.J. Madrid. 2003. pág. 278.

[47] Así es de recordar el asunto objeto del auto de la Audiencia Nacional de 19 de mayo de 1999 por el que se denegó la extradición de un ciudadano alemán a Hungría, que había instalado un sistema de llamadas telefónicas internacionales alterado mediante un programa informático, con el que logró defraudar a la Compañía Húngara de Telecomunicaciones un equivalente a los 44 millones de pesetas, y que mientras que para la legislación penal húngara constituía un delito grave, de fraude informático, para la española, a tenor de la interpretación de la Audiencia Nacional, era una mera defraudación de fluido eléctrico o

llamados **"paraísos informáticos"**, auténticos reinos de impunidad para el delincuente por internet. La situación puede llegar a producir una verdadera impunidad, si no se articulan los remedios adecuados[48].

4. El gran número de usuarios, las frecuencias de acceso y uso, así como la libre circulación y navegación tanto para emitir, trasferir y difundir información como para acceder a ella por medio de la red, permite que los cibernautas puedan ser al mismo tiempo potenciales víctimas como perpetradores de los hechos ilícitos.

5. Facilita el anonimato, tanto para los delincuentes con conocimientos técnicos que pueden recurrir a la utilización de herramientas para la navegación anónima[49], como también para aquellos que carecen de esos conocimientos técnicos, pues les otorga cierto y relativo anonimato cuando operan a gran distancia detrás de un número IP, dirección de correo electrónico o perfil, ya que a menudo no es fácil rastrear a un individuo específico. Aunque pudiera seguirse el rastro digital dejado al iniciar la comunicación y proseguir la navegación y accesos correspondientes, hasta conocer desde qué terminal y a través de qué servidor se operó en la red, no es tan fácil identificar el individuo concreto que realmente lo perpetró[50].

6. Permite la interacción distante con las víctimas, eliminando posibles barreras sociales que los delincuentes encuentran en la interacción de persona a persona. La ciberdelincuencia implica por lo tanto "las relaciones anónimas entre perpetradores y víctimas"[51].

---

análogo, delito menor y por tanto no susceptible de extradición (*Vid.* ROVIRA DEL CANTO, E. "Delincuencia informática y fraudes informáticos*"*. Ed. Comares, Granada, 2002. págs. 648 y 649).

[48] DÍAZ GÓMEZ, A. "El delito informático, su problemática y la cooperación internacional (…)". ob. cit. págs. 169-203.

[49] Como proxy, remailers y redes torrents.

[50]ROMEO CASABONA, C. M. *De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal*, en "El cibercrimen: nuevos retos jurídico-penales*,* nuevas respuestas político-criminales" (Romeo Casabona, coord). Ed. Comares, Granada, 2006, pág. 3.

[51] SANDYWELL, BARRY. *On the globalisation of crime: the internet and new criminality*. En "Handbook of internet crime". (Yvone Jewkes and Majid Yard, coord.). Ed. Willan Publishing, Portland USA, 2010, pág. 44.

7. Las propias características físicas, técnicas y lógicas facilitan la manipulabilidad de datos y el software con un costo mínimo, ya que se basa en la representación digital (lo que permite la copia sin pérdida de calidad, y la alteración sin huellas visibles)[52]. De este modo, puede conseguirse el acceso a ficheros y archivos de muy variada naturaleza y trascendencia sin autorización de sus titulares, la manipulación de sus contenidos por diversos procedimientos, incluida la alteración del software conforme a las necesidades o propósitos del intruso. Así, se afirma que *"lo real puede convertirse en falso, el original en copia y el ser en identidad virtual"*[53].

8. Permite la automatización en la comisión del delito[54], en aquellos casos en los que un virus es lanzado a internet puede replicar y atacar a millones de ordenadores al mismo tiempo, pero también a lo largo de períodos de tiempo, e incluso personalizarse para crear un nuevo virus[55].

9. Puede generar un daño de mayor escala y de mayor consideración (por ejemplo, cuando una fotografía es publicada en la red adquiere un alcance global y un impacto mucho mayor que por cualquier otro medio).

---

[52] SANDYWELL, BARRY. *On the globalisation of crime: the internet* (…) ob. cit. pág. 44.

[53] MORÓN LERMA, E. "Internet y Derecho Penal: Hacking y otras Conductas Ilícitas en la Red", colección RdPP monografía. Ed. Aranzadi, Pamplona, 1999, pág. 79.

[54] ROVIRA DEL CANTO, E. "Delincuencia informática y (…)". ob. cit. pág. 650. Efectivamente, la incidencia de la posibilidad de repetición de una actuación ilícita en el ámbito informático, telemático y cibernético, favorece su nueva comisión, incluso en múltiples ocasiones, derivando en la práctica a que en un alto porcentaje de los supuestos conocidos y enjuiciados de ilícitos informáticos la conducta de los autores no se ha limitado a una única acción delictual, sino a una reiteración continua de la misma. Pero es que, además, cabe la realización de una sola inicial acción por parte del sujeto activo, consistente en una manipulación del programa de funcionamiento informático, o un cambio en la base de datos, es decir afectar a las funciones de almacenamiento, procesamiento y transferencia de datos o de la información, para que la frecuente repetición del hecho delictivo provenga no de diversas acciones individuales del autor sino de un *automatismo del sistema*, sin intervención alguna del sujeto activo, puesto que variada o creada una nueva instrucción en el programa informático correspondiente, cada vez que se acceda al programa o a la base de datos, el sistema va a repetir automáticamente la manipulación.

[55] WALL, DAVID S. *Criminalising cyberspace: the rise of the internet as a crime problem.* En "Handbook of internet crime". (Yvone Jewkes and Majid Yard, coord.). Ed. Willan Publishing, Portland USA, 2010, pág. 99.

10. Puede atacar a diversas víctimas pero ocasionar a cada una de ellas un daño muy pequeño (como por ejemplo, a través de las técnicas por las cuales se sustrae 0,5 céntimos de euro de diez mil cuentas bancarias diferentes mil veces). Este problema de *minimis* puede ser uno de los mayores retos de la ciberdelincuencia ya que reduce los incentivos para informar, investigar y enjuiciar el delito[56].

11. Facilita o magnifica la comisión de delitos cuyo injusto viene fundamentado en los contenidos de la información, como son los casos de apología del terrorismo, la discriminación de determinados grupos de personas, la xenofobia, la comisión de injurias contra terceros, la difusión de pornografía infantil, la distribución e intercambio no autorizado de obras de creación intelectual etc… Internet no solo facilita la difusión por sus características, sino también debido a que abarata los costes de difusión al tiempo que favorece la comunicación y el intercambio entre personas afines (ej. pornografía infantil)[57].

12. Internet facilita el comercio de la información que se ha convertido en un activo valioso tanto en el mercado legal (música, películas, software, libros) como en el mercado negro, donde los números de tarjetas de crédito, información personal y contraseñas se comercializan para facilitar el fraude y el robo[58]. Incluso se ha convertido internet en un medio a través del cual se realizan acciones de ciberguerra[59] y ciberespionaje[60].

---

[56] WALL, DAVID S. "Cybercrime: The transformation of crime in the information age". Ed. Cambridge, polity press, UK, 2007. pág. 10.

[57] ROMEO CASABONA, C. M. *De los delitos informáticos al cibercrimen* (…) ob. cit. pág. 4.

[58] WALL, DAVID S. Cybercrime: The transformation of crime (…) ob. cit. pág. 32.
ABC tecnología, 22/09/2016. La compañía estadounidense *Yahoo* confirmó en 20016 el robo de 500 millones de cuentas, y acusó a un grupo probablemente ligado a un Estado de estar detrás de uno de los mayores "hackeos" de datos de la historia. El ataque tuvo lugar a finales de 2014, y afectó a las direcciones de correo electrónico, números de teléfono, fechas de nacimiento y contraseñas pero no datos de tarjetas de pago, según la compañía estadounidense.
ABC tecnología 19/05/2016. *LinkedIn***,** hackeada, recomienda a los usuarios a cambiar la contraseña. Medios estadounidenses aseguran que el autor del robo es el mismo "hacker" que consiguió burlar la seguridad de la red profesional en 2012. Ahora vende en la "Depp Web" las claves de acceso.

[59] El ciberespacio ha sido declarado por la ONU (Estrategia Nacional Militar de la NU para las operaciones del Ciberespacio de 2006) como el próximo escenario de los conflictos bélicos, además de la tierra, el aire, el mar y el espacio.

13. La estructura descentralizada y no jerarquizada de la red es incompatible con la existencia de órganos o instituciones que controlen la cantidad información que circula en la red lo que imposibilita o dificulta filtrar, supervisar o controlar dicho volumen de información.

14. Su innovación constante permite nuevas técnicas y herramientas que se desarrollarán con el objetivo de burlar las medidas de seguridad existentes y cometer nuevos delitos.

15. Desde el punto de vista de la prueba, se dificulta su obtención por el carácter intangible de los datos y de la información que contienen y por el carácter eminentemente volátil al estar en un espacio virtual y en un sistema de continua transferencia y transmisión que permite su supresión, alteración, transformación u ocultación en cualquier momento. También porque presenta serias dificultades para lograr la conservación o almacenamiento de los datos en un soporte. Y porque aún en este caso, la falta de visualización de los datos almacenados electromagnéticamente dificulta de forma considerable la acreditación del ilícito, pues cualquiera que quisiera comprobarlos y revisarlos no puede hacerlo directamente sobre los datos, sino que siempre debe acudir a los términos del ordenador y a las comunicaciones a través de la pantalla, que además, pueden haber sido objeto de manipulación[61].

Aunque los autores tienden a señalar estos factores de riesgo como las principales causas a tener en cuenta, por lo general, existe acuerdo en que es su combinación lo que hace que la ciberdelincuencia sea un reto especial que produce cambios en la delincuencia ordinaria. En definitiva, el Derecho penal se enfrenta a una

[60] EFE 5/9/2016. El presidente de Estados Unidos, Barack Obama, aseguró que internet no puede convertirse en el salvaje Oeste, en referencia al ataque de piratas informáticos ligados al Gobierno ruso contra la red del Comité Nacional Demócrata en una operación de espionaje.

[61] ROVIRA DEL CANTO, E. "Delincuencia informática y (…)" ob. cit. pág. 295. Este problema ha sido denominado por la criminología americana como "*Secondhand*".

criminalidad progresivamente más peligrosa a la que el Derecho procesal debe dar también la respuesta necesaria[62].

[62] TEJADA DE LA FUENTE, E. La retención obligatoria de datos de tráfico de las comunicaciones electrónicas y telemáticas y la preservación específica de datos informáticos como herramientas de investigación criminal. En "El Derecho de Internet" (Pérez Bes, Coord). Ed. Atelier, Barcelona, 2016. pág. 316. "*La respuesta del Estado de derecho ante esa nueva criminalidad no solamente precisa de la articulación de nuevos tipos penales. Hay otro aspecto que en ningún caso puede descuidarse que es el relacionado con la investigación criminal."*

CAPÍTULO SEGUNDO

CONCEPTO DE CIBERDELITO, CLASES Y TÉCNICAS DE COMISIÓN.

1. APROXIMACIÓN AL CONCEPTO.

Desde un punto de vista jurídico, el primer problema a la hora de afrontar el análisis de los ciberdelitos es intentar describir su contenido. Así, la primera dificultad es precisamente su conceptualización[63]. No existe un concepto dogmático de delito informático ni de cibercrimen o ciberdelito, ni tampoco puede construirse de *lege data* en el derecho español[64]. La doctrina ha debatido durante años si nos encontramos ante una categoría que pueda denominarse ***"ciberdelito o delito informático"*** o si, por el contrario, se deben utilizar expresiones que carezcan de un matiz jurídico-positivo, haciendo alusión, más bien, a categorías criminológicas, como pueden ser las expresiones delincuencia informática, ciberdelincuencia o criminalidad informática[65].

En la actualidad hay una amplia gama de adjetivos usados para describir los delitos cometidos por internet o haciendo uso de nuevas tecnologías, sean delitos informáticos, ciberdelitos, delitos telemáticos, cibernéticos, en línea u *on line*, digital, en red, de alta tecnología, relacionados con internet, relacionados con la informática, relacionados con las telecomunicaciones, asistidos por ordenador, electrónicos etc (...).

---

[63] ORTEGA GUTIÉRREZ-MATURANA, M. "Ilícitos militares cometidos a través de internet o con ocasión del uso de las nuevas tecnologías (i). Delimitación y problemas procesales y de prueba que plantean". Ponencia presentada en las Jornadas de la Fiscalía Jurídico Militar, año 2013. Pág. 10 https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Marcelo%20Ortega%20Gutierrez-Maturana.pdf?idFile=1bf8666f-ba3e-40ae-9129-4dec942c381c.

[64] ROMEO CASABONA, C. M. *De los delitos informáticos al cibercrimen* (…) ob. cit. pág. 1-42.

[65] YAR, MAJID. "The Novelty of 'Cybercrime". European Society of Criminology and SAGE Publications London, Thousand Oaks CA, and New Delhi, 2005. pág. 409 "*Un problema principal para el análisis de la ciberdelincuencia era la ausencia de una definición consistente, incluso entre los organismos encargados de hacer cumplir la ley y de hacerle frente (NHTCU / NOP 2002: 3).*

De entre todos los términos acuñados, y aunque cualquiera de ellos podría haber sido justificadamente elegido, estimo preferible optar por el de **ciberdelito,** pues dicho término, aunque no se encuentre en el diccionario de la Real Academia de la Lengua Española[66], permite de una parte englobar todos los delitos cometidos por internet o en los que la red esté siempre de una forma u otra involucrada en la comisión de los mismos, pero al mismo tiempo comprende determinadas conductas delictivas relacionadas con la informática para cuya producción no se haya hecho uso de internet[67]. Otra razón por la que opto por el término ciberdelito es que es la traducción española más correcta del nombre en inglés aceptado internacionalmente y recogido en el Convenio del Consejo de Europa sobre "*Cibercrime*", hecho en Budapest el 23 de noviembre 2001. También el Tribunal Supremo ha hecho uso de este vocablo en sus resoluciones[68]. De ahí el uso del término "ciberdelito" en lo sucesivo.

No resulta fácil determinar qué debe entenderse por ciberdelito y sobre todo qué conductas puedan considerarse incluidas. Tampoco la doctrina ha encontrado un concepto unitario de delito informático y las discrepancias en torno al mismo han llegado a propiciar que algunos autores admitan la imposibilidad de dar una definición precisa renunciando a ello[69]. Este es uno de los motivos por los que prescindo de usar la expresión de delito informático, pues en la actualidad existe una concepción muy amplia del mismo, cuando en realidad si se analiza detenidamente los diferentes tipos

[66] La última edición es la 23ª publicada en octubre de 2014. http://"lema.rae.es/drae/?val=ciberdelito. Si se encuentra el término **ciber-** que indica relación con las redes informáticas. Como vocablos ya admitidos están los de ciberespacio, cibernauta, cibernético/a.

[67] Piénsese, por ejemplo, en aquellos casos en los que causan daños a un sistema informático a través de un virus que es introducido en un ordenador a través de un USB y no a través de la red.

[68] ATS 19 de febrero de 2014 (Sección 1ª), que resuelve una cuestión de competencia de un "*ciberdelito conocido como phising"*. ATS de 29 de octubre de 2015 (sección 1ª) que hace referencia a una modalidad de "ciberdelito" muy extendida consistente en extorsionar a personas que previamente habían sido grabadas practicando *cibersexo*.

[69] HERNÁNDEZ DÍAZ, L. "El Delito Informático". Cuaderno del Instituto Vasco de Criminología nº 23, 2009, págs. 227-243. En el mismo sentido, FERREYROS SOTO, C. *Aspectos metodológicos del delito informático*, en "Informática y derecho". Revista iberoamericana de derecho informático nº 9-11, 1996, págs. 407 prescinde de una conceptuación, limitándose a enumerar las peculiaridades que presenta el conjunto de comportamientos a que puede venir referida la expresión.

penales se puede discrepar en no pocos casos de la idoneidad de incorporar el adjetivo "informático" a muchos de los delitos en cuestión[70].

Parece existir una categoría criminológica que puede denominarse criminalidad informática o delincuencia informática que incluye todas las conductas sancionadas por el Código Penal que tengan vinculación con la informática bien en su medio comisivo, bien en el objeto sobre el que recae la conducta, bien en ambos u otros ilícitos que en su momento puedan entrar a formar parte de él. Pero también es posible, y parece que aconsejable, insistir en el estudio sobre la conveniencia de proteger también un nuevo bien jurídico vinculado a lo informático, que todavía no aparece claramente definido en la legislación penal pero a favor del cual parece apostar cada vez más la doctrina que se ha detenido en estas cuestiones[71].

Así, internet y las redes telemáticas traen consigo un nuevo concepto superador del tradicional de delito informático, como es el de **ciberdelito**[72]. Cuando se habla de ciberdelito se hace referencia a un tipo de delito, ya sea tradicional o propio de la sociedad de la información, propiciado por las tecnologías que ésta aporta[73], fundamentalmente internet. Pero no se refiere a cualquier conducta delictiva en cuya

[70] GONZÁLEZ HURTADO, J.A. "Delincuencia informática: daños informáticos del artículo 264 del código penal y propuesta de reforma". Tesis doctoral, Universidad Complutense de Madrid, departamento de derecho penal, Madrid, 2013. pág. 134.

[71] HERNÁNDEZ DÍAZ, L. "El Delito Informático (…)" ob. cit pág. 241.

[72] Es con el X Congreso de las Naciones Unidas sobre la Prevención del Delito y el Tratamiento del Delincuente, celebrado en Viena del 14 al 17 de abril de 2000, se partió de un concepto del delito cibernético como "todo delito que puede cometerse por medio de un sistema o una red informáticos, en un sistema o una red informáticos o contra un sistema o una red informáticos", abarcando, en principio, "todo delito que puede cometerse en un medio electrónico", y utilizando la palabra "delitos" para designar "formas de comportamiento generalmente definidas como ilegales o que probablemente serán declaradas ilegales en breve plazo", siendo posible que determinada conducta estuviera tipificada como delito en un Estado y no en otros, pero sobre el sentido dado en un entendimiento común internacional en cuanto al tipo de comportamiento relacionado con los sistemas y redes informáticos que debe declararse ilegal. En tales términos establece dos subcategorías de delitos cibernéticos: a) Delito cibernético en sentido estricto ("delito informático"): todo comportamiento ilícito que se valga de operaciones electrónicas para atentar contra la seguridad de los sistemas informáticos y los datos procesados por ellos; b) Delito cibernético en sentido lato ("delito relacionado con ordenadores"): todo comportamiento ilícito realizado por medio de un sistema o una red informáticos, o en relación con ellos; incluidos los delitos como la posesión, el ofrecimiento o la distribución ilegales de información por medio de un sistema o una red informáticos. ROVIRA DEL CANTO, E. "Hacia una expansión doctrinal y fáctica del fraude informático". Revista Aranzadi de Derecho y Nuevas Tecnologías nº 2003-3, Pamplona, 2003, págs 115 y 116.

[73] DE URBANO CASTRILLO, E. "Los delitos informáticos tras la reforma del CP de 2010". Revista Aranzadi Doctrinal nº 9, parte Estudio. Pamplona. 2011, pág. 1.

ejecución se haga uso de internet, pues ello daría lugar a una desnaturalización del concepto.

El art. 14 del Convenio sobre Ciberdelincuencia ofrece una idea de su complejidad, al establecer que el ámbito de aplicación de sus normas procesales se refiere a todas las conductas con apariencia criminal, siempre que se hallen en un entorno de comisión delictiva en el que los medios informáticos hayan desempeñado un papel relevante. Se toma en cuenta por tanto la utilización de sistemas y datos informáticos en tres diferentes perspectivas:

a) como objeto mismo sobre el que se produce el delito
b) como instrumento para la comisión delictiva
c) como simple soporte de información.

Si este último aspecto se conecta con las definiciones de sistema y datos informáticos establecidas por el art. 1 del mismo Convenio y se repara en el índice de penetración que éstos tienen en la sociedad de nuestros días, fácilmente se llega a la conclusión de que una gran mayoría de delitos podrían entrar en la categoría de delitos informáticos[74].

El término ciberdelito se entiende pues como "el conjunto de conductas relativas al acceso, apropiación, intercambio y puesta a disposición de información en redes telemáticas, las cuales constituyen su entorno comisivo, perpetradas sin el consentimiento o autorización exigibles o utilizando información de contenido ilícito, pudiendo afectar a bienes jurídicos diversos de naturaleza individual o supraindividual"[75]. Estaríamos ante una nueva generación de delitos, que en lugar de tener una vinculación con los sistemas informáticos, se caracterizan por el uso de redes de transmisión de datos, siendo su relación con los sistemas informáticos secundaria respecto a la que tienen con las redes de transmisión de datos.

[74] PÉREZ GIL, J. "Investigación penal y nuevas tecnologías: algunos de los retos pendientes". Revista jurídica de Castilla y León nº 7, octubre 2005, pág. 223.

[75] ROMEO CASABONA, C. M. *De los delitos informáticos al cibercrimen* (…) ob. cit. pág. 11. "*Algún autor, como TOSATO, "Panorama di giurisprudenza sui reati informatici", p. 446, ha utilizado, en lugar de la expresión "ciberdelito", el término "delito cuasinformático" para referirse a la misma realidad delictiva".*

De ahí que el término ciberdelito resulte idóneo para referirse un gama de actividades ilícitas cuyo denominador común es el papel central que desempeñan las redes de información y la comunicación (TIC) en su comisión.

Una definición aproximada conceptualiza la ciberdelincuencia como "*las actividades mediadas por ordenador que son ilegales y que pueden llevarse a cabo a través de las redes"*[76]. El ciberdelito se presenta no solo como manifestación global y genérica de la criminalidad informática originada por el riesgo propio del uso y utilización de la informática, la telemática y de la información en la actual sociedad, sino además como concepto comprensivo de un conjunto de figuras sustantivas y normativas de tipos delictivos con entidad y sustantividad propia que conformarían el núcleo de lo que se ha venido formulando como Derecho penal global del riesgo informático, en el que el ciberdelito viene configurado como un delito pluriofensivo, en el que hay que tener siempre concurrente la protección de los nuevos intereses derivados de la sociedad global de la información (la información en sí misma, los datos informáticos, que son la representación de aquella, y la fiabilidad y seguridad colectiva en los medios y sistemas de tratamiento y transferencia de la información).

2. CLASIFICACIÓN DE LOS CIBERDELITOS.

A efectos de una mayor claridad expositiva, procederé a efectuar una triple distinción y a examinar, en concordancia con ella, cada una de la clasificaciones aportadas en la doctrina, en las instituciones y en las normas. Todas estas clasificaciones responden a muy diversas formas de interpretar el contenido de este tipo de delitos.

2.1 Clasificación doctrinal .

La clasificación más común en la doctrina internacional es la que distingue entre internet como una herramienta o como un objetivo[77]. Además de las redes de

[76] THOMAS, D Y LOADER B. "Cybercrime: law enforcement, security and surveillance in the information age". Ed. Cambridge University Press. Routledge, London, 2000. pág. 3.

[77] KOOPS, BERT-JAAP. *The internet and its opportunities* (…) ob.cit. págs. 735-754.

ordenadores y sistemas como instrumento u objeto del delito, se ha señalado un tercer tipo, donde internet es el "medio ambiente" de la delincuencia, en el sentido de un fondo más o menos neutro para un cometer un delito[78]. Una de las primeras definiciones habla de los *abusos informáticos*[79] y lo define como "cualquier incidente asociado con la tecnología de los ordenadores en el que la víctima sufrió o pudo haber sufrido un daño y el autor, intencionadamente, obtuvo o pudo haber obtenido un beneficio"[80].

Algunos autores fijan el concepto teniendo en cuenta el modo en el que participan las Tecnologías de la Información y Comunicación[81]. Un sector doctrinal[82] distingue entre el concepto en sentido estricto (que incluye todos los delitos en los que las TIC son usadas como medio y como objetivo del delito, tales como la piratería informática o la propagación de virus informáticos etc….) y el concepto en sentido amplio (que incluye los delitos donde las TIC son esenciales para la ejecución pero no son el objetivo)[83]. Dentro de este concepto amplio es fundamental distinguir entre aquellos delitos en los que el uso de las TIC es esencial para la ejecución, de aquellos en los que es solo una herramienta, porque estos últimos no entran técnicamente en el

---

https://pure.uvt.nl/portal/files/1290818/Koops_The_Internet_and_its_opportunities_for_cybercrime_110105_postprint_immediately.pdf.

[78] SMITH RUSSEL G, GRABOSKY PETER, URBAS GREGOR. "Cyber Criminals on Trial". Ed. Cambridge University Press. Cambridge, 2011. págs 5 a 7.

[79] PARKER , D.B. "Computer Abuse: Final Report". Ed. National Technical Information Service. USA 1973. PARKER , D.B. "Crime by computer". Ed. Charles Scribner´s son. New York. 1976. págs.12 ss. y 237 ss. Este autor no se limitó a describir las conductas relevantes para el ámbito penal sino que reconoce que se trata de un amplio abanico de conductas en las que se incluyen además de conductas de naturaleza penal, otras de relevancia civil y meros incidentes sin trascendencia jurídica. A pesar de la vertiente patrimonial de su estudio, el autor también se preocupó por los ataques a la intimidad que, con la creación de las primeras bases de datos, podían derivarse de la digitalización de datos de naturaleza privada.

[80] KOOPS, BERT-JAAP. *The internet and its opportunities* (…) ob. cit. págs. 735-754.

[81] La Comisión Europea en el año 2007 definió la ciberdelincuencia como "*actos criminales cometidos utilizando redes de comunicación y los sistemas de información electrónicos o contra este tipo de redes y sistemas" vid.* Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité de la Regiones: hacia una política general de lucha contra la ciberdelincuencia. (COM(2007) 267 final de 22.5.2007).

[82] STOL, WOUTER. *Cyberspace and safety. "*Cyber Safety: An Introduccion" (Leukfeldt & Stol). Ed. Eleven International Publishing. Holanda, 2012 pág. 23. KOOPS, BERT-JAAP. *The internet and its opportunities* (…) ob.cit. págs. 735-754. SMITH RUSSEL G, GRABOSKY PETER, URBAS GREGOR. "Cyber Criminals on Trial (…)" ob. cit. págs. 5 a 7.

[83] Los delitos tradicionales en los que se usan las TIC son llamados *old wine in a new bottle*. *Vid.* GRABOSKY P. "Virtual Ciminality: old wine in New Bottles?" Social Legal Studies y SAGE Publication, London 2001 págs. 243 a 249.

concepto de ciberdelito (piénsese, por ejemplo, en el delincuente que usa google maps para buscar una ruta por la que escapar).

Otra clasificación[84] se centra en la estructura de oportunidades que ofrece la evolución de la ciberdelincuencia, distinguiendo desde este punto de vista tres generaciones:

1) La primera generación consiste en delitos tradicionales donde los ordenadores no son más que una herramienta constituyendo una 'gama baja' de ciberdelitos.

2) La segunda, consta de delitos facilitados por redes informáticas locales o globales; éstos siguen siendo en gran medida los delitos tradicionales, pero dan lugar a nuevas oportunidades por ese alcance globalizado.

3) La tercera, son verdaderos delitos totalmente mediados por la tecnología, lo que constituye un cambio en la transformación de la ciberdelincuencia. Estos son 'gama alta' y sui generis de los ciberdelitos que no existirían sin internet. No es el foco de esta tipología tanto el papel de internet como herramienta u objetivo, sino la forma en la que el delito en sí se está transformando por internet y evolucionando hacia nuevas formas con diferentes modelos de organización del delincuente y distintas las relaciones delincuente-víctima[85].

Incluso ya se plantea la cuestión de si está surgiendo una cuarta generación, donde el ciberdelito ocurre no sólo a través de, o en, internet, sino en espacios totalmente virtuales, como puede ser en los juegos multi-jugador en línea (por ejemplo, World of Warcraft) y en mundos virtuales (por ejemplo, Second Life)[86]. Se plantea la cuestión de si estamos en presencia o no de una cuarta generación de "delito virtual", o simplemente como una nueva forma de cometer delitos tradicionales (segunda

[84] WALL, DAVID S. Cybercrime: The transformation of crime (…) ob. cit. págs. 44-48.

[85] WALL, DAVID S. Criminalising cyberspace: the rise of the internet as a crime problema. En "Handbook of internet crime". (Yvone Jewkes and Majid Yard, coord.). Ed. Willan Publishing, Portland USA, 2010 págs. 94 a 97.

[86] En caso de abuso cometido en estos espacios virtuales. Piénsese, por ejemplo, en el robo de espadas virtuales, tener relaciones sexuales con un joven avatar, o abusar virtualmente de un menor, que pueden ser tratados como un nuevo tipo *sui generis* de la delincuencia.

generación), o no estamos en presencia de un delito en absoluto ya que es sólo "virtual" y no "real". Solo si hay alguna manifestación en el mundo real, alguna forma de daño real (es decir, no virtual) el comportamiento podrá ser tratado como un delito. Precisamente, con el fin de solucionar los problemas de falta de tipicidad de algunas de estas conductas, la reforma del Código Penal operada por Ley Orgánica 1/2015, de 30 de marzo introdujo en materia de pornografía infantil, una definición legal de la misma tomada de la Directiva 2011/93/UE, que abarcaba no sólo el material que representa a un menor o persona con discapacidad participando en una conducta sexual, sino también las imágenes simuladas de menores participando en conductas sexualmente explícitas, aunque no reflejen una realidad sucedida[87].

Otra clasificación doctrinal interesante[88] es la basada en las distintas motivaciones a la hora de cometer el delito. Así, se distingue entre los hackers y phreakers (motivados por la curiosidad), los comerciantes de la información y mercenarios (motivados por la ganancia financiera), y los terroristas y extremistas (motivados por política o actividad social).

Otros autores distinguen entre delito informático (un concepto singular de delito que podría abarcar nuevos delitos perpetrados en nuevas formas) y delito cibernético (un término descriptivo para un tipo de delito que implique delitos convecionales perpetrados utilizando las nuevas tecnologías)[89].

En España, VELASCO NÚÑEZ[90], acoge un concepto amplio de ciberdelito que incluye tanto el delito tradicional cometido a través de internet (injurias a través de

[87] Art. 189 CP *"(...) Se considera pornografía infantil o en cuya elaboración hayan sido utilizadas personas con discapacidad necesitadas de especial protección: (...)*

c) *Todo material que represente de forma visual a una persona que parezca ser un menor participando en una conducta sexualmente explícita, real o simulada, o cualquier representación de los órganos sexuales de una persona que parezca ser un menor, con fines principalmente sexuales, salvo que la persona que parezca ser un menor resulte tener en realidad dieciocho años o más en el momento de obtenerse las imágenes.*

d) Imágenes realistas de un menor participando en una conducta sexualmente explícita o imágenes realistas de los órganos sexuales de un menor, con fines principalmente sexuales."

[88]THOMAS, D Y LOADER, B. Cybercrime: law enforcement (…) ob. cit. pág. 3.

[89] SMITH RUSSEL G, GRABOSKY PETER, URBAS GREGOR. "Cyber Criminals on Trial (…) ob. cit. págs. 5 a 7.

[90] VELASCO NÚÑEZ, E. "Delitos cometidos a través de Internet. Cuestiones Procesales*"*. Ed. La Ley-Actualidad, Madrid, 2010. pág. 41.

correo electrónico, venta de droga, extorsión o amenazas vehiculizadas a través de Internet, etc.), como el propiamente tal, delito contra la informática -por atacar los datos o sistemas informáticos o las vías telemáticas de comunicación, especialmente a través de Internet-, ya sea bloqueando sistemas (ataques de denegación de servicio o DDoS), destruyendo programas, dañando dispositivos de almacenamiento, alterando datos (fraude), destruyéndolos (sabotaje) o usándolos ilícitamente (piratería, espionaje).

La doctrina española mayoritaria[91], admite como más adecuada la clasificación tripartita de los delitos, que se desarrolla a continuación, relacionándola con su calificación jurídica en el Código Penal.

1. Ciberdelincuencia económica: delitos económico-patrimoniales vinculados a la informática.

Se trata de los ataques al bien jurídico patrimonio ajeno vehiculizados a través de la informática, siempre realizados con la intención, por cualquier medio, de consumar apoderamientos o beneficios económicamente evaluables sobre el patrimonio de terceras personas. Constituyen la mayor parte de los delitos informáticos que se denuncian. En el Código Penal principalmente son el robo inutilizando sistemas de guardia criptográfica (art. 238.5CP), la estafa informática (art. 248.2 CP), la defraudación de telecomunicaciones informáticas (art. 255CP), el uso no autorizado de terminales informáticos (art. 256 CP), daños informáticos (art. 264.2 CP), estragos informáticos (art. 346 CP), contra la propiedad intelectual informática (art. 270.3 CP) o industrial informática (art. 273-275 CP), espionaje informático de secretos de empresa (art. 278-280CP), la publicidad engañosa (art. 282 CP), manipulaciones en aparatos en perjuicio del consumidor (art. 283 CP), delitos contra el mercado informático (art. 286 CP), blanqueo informático de capitales (art. 301 CP) y falsedad documental en soporte electrónico (art. 390 en relación con el artículo 26 CP).

2. Ciberdelincuencia intrusiva: atentados por medios informáticos contra la intimidad y la privacidad. Se trata de los ataques al bien jurídico privacidad como un

[91] VELASCO NÚÑEZ, E. "Delitos cometidos a través de Internet. Cuestiones Procesales". ob. cit. pág. 42. HERRERO-TEJEDOR ALGAR, F. "Capítulo VIII. Delitos Informáticos". Cuaderno de derecho para ingenieros. Cuaderno Duodédimo: La Nueva Reforma del Código Penal.volumen 12, año 2012, pág. 144 y 145. ORTEGA GUTIÉRREZ-MATURANA, M. "Ilícitos militares cometidos a través de internet o con ocasión del uso de las nuevas tecnologías (i) (…)". ob. cit. pág. 11.

concepto que, incluyendo el de intimidad, va más allá, pues abarca todas las modalidades protegidas en el art. 18 CE (el honor, la intimidad personal, la familiar, la propia imagen, el domicilio, el secreto de las comunicaciones o el uso correcto de la informática).

Estos suponen una cuarta parte de los delitos que se denuncian y, entre otros, se encuentran tipificados en el Código Penal las amenazas y coacciones informáticas (arts. 169 y 172 CP), la distribución de material pornográfico y pornografía infantil (art. 186 a 189 CP), el descubrimiento *y* revelación de secretos (art. 197 CP), las injurias *y* calumnias informáticas (arts. 205-216 CP) y la cesión no consentida de datos ajenos (arts. 417, 418 y 423 CP).

3. Ciberespionaje y Ciberterrorismo: ataques por medios informáticos contra intereses supraindividuales. Se trata de los ataques más graves, que afectan indiscriminadamente a intereses generales de la población con la intención de crear pánico y terror para subvertir el sistema político o de convivencia generalmente aceptado. Apenas tienen incidencia estadística, pero su realización, por afectar a la población en general, genera una alta intranquilidad y desasosiego. También cabría incluir dentro de este grupo, la usurpación de funciones públicas (art. 402 CP) o el descubrimiento y revelación de secretos relativos a la defensa nacional (arts. 598 y 603 CP).

En mi opinión considero que aún cabe realizar una clasificación todavía más reduccionista, por lo que distingo dos tipos:

a) ciberdelito "stricto sensu", como la intrusión en equipos ajenos (hacking), la revelación de contenidos albergados en programas y archivos informáticos, los fraudes (phising y pharming), la falsificación informática, y los daños a los elementos lógicos del sistema (cracking)

b) delitos clásicos que encuentran en la red su medio comisivo (así, las amenazas, las vejaciones, el ciberterrorismo, los delitos contra la libertad sexual...).

2.2 Clasificación institucional.

Partiendo del modo en el que participan las tecnologías de la información y comunicación, la Fiscalía General del Estado en *la Instrucción 2/2011, del Fiscal de Sala de criminalidad informática y las secciones de criminalidad informática de las Fiscalías*,[92] establece una clasificación de delitos intentando diferenciar los delitos informáticos en sentido estricto[93] de aquellos otros delitos en los que la informática simplemente aparece de forma incidental.

Se establece un catálogo inicial de delitos informáticos[94] en los que intervendrán fiscales especializados, pero sin limitar en un *numerus clausus* los tipos penales

[92] Instrucción de la Fiscalía General del Estado, *Instrucción 2/2011, del Fiscal de Sala de criminalidad informática y las secciones de criminalidad informática de las Fiscalías"*. Pág. 4 *(...)* el área de especialización en criminalidad informática surge como una necesidad constatada en la práctica habitual de las Fiscalías al haberse detectado un progresivo aumento en el número de investigaciones criminales vinculadas a la utilización de las nuevas tecnologías y más específicamente de internet, como red de redes.

[93] Delitos en los que el objeto de la actividad delictiva son los propios sistemas informáticos o las TIC.; aquellos en los que la actividad criminal se sirve para su ejecución de las ventajas que ofrecen las TICs; y aquellos en los que la actividad criminal, además de servirse para su ejecución de las ventajas que ofrecen las TIC, entraña especial complejidad en su investigación que demanda conocimientos específicos en la materia; así como finalmente cualquier otro tipo delictivo en cuya ejecución haya sido determinante la utilización de las TICs y en los que dicha circunstancia genere una especial complejidad en la investigación criminal.

[94]Instrucción de la Fiscalía General del Estado, *Instrucción 2/2011, del Fiscal de Sala de criminalidad informática y las secciones de criminalidad informática de las Fiscalías"*. págs. 7 y 8.

2. A) Delitos en los que el objeto de la actividad delictiva son los propios sistemas informáticos o las TICs.

-Delitos de daños, sabotaje informático y ataques de denegación de servicios previstos y penados en el artículo 264 y concordantes del Código Penal.

-Delitos de acceso sin autorización a datos, programas o sistemas informáticos previstos y penados en el artículo 197.3 del Código Penal.

-Delitos de descubrimiento y revelación de secretos del artículo 197 del Código Penal cometidos a través de las TICs o cuyo objeto sean datos que se hallen registrados en ficheros o soportes informáticos electrónicos o telemáticos.

-Delitos de descubrimiento y revelación de secretos de empresa previstos y penados en el artículo 278 del Código Penal cometidos a través de las TICs o cuyo objeto sean datos que se hallen registrados en ficheros o soportes informáticos ó electrónicos.

-Delitos contra los servicios de radiodifusión e interactivos previstos y penados en el artículo 286 del Código Penal.

2. B) Delitos en los que la actividad criminal se sirve para su ejecución de las ventajas que ofrecen las TICs.

-Delitos de estafa previstos y penados en el artículo 248.2 a) b) y c) del Código Penal, siempre que, en los supuestos a) y c) se utilicen las TICs para llevar a efecto la transferencia u operación de cualquier tipo en perjuicio de otro.

-Delitos de acoso a menores de 13 años, *child grooming*, previstos y penados en el art. 183 bis del Código Penal cuando se lleve a efecto a través de las TICs.

-Delitos de corrupción de menores o de personas discapacitadas o relativas a pornografía infantil o referida a personas discapacitadas previstos y penados en el artículo 189 del Código Penal cuando para el desarrollo y/o ejecución de la actividad delictiva se utilicen las TICs.

susceptibles de encuadrarse en la categoría de criminalidad informática[95], pues según la propia Instrucción (…) "*es más que previsible la aparición, en un futuro más o menos próximo, de nuevas formas de delincuencia o nuevos mecanismos de comisión de ilícitos ya tipificados, en los que el elemento determinante sea también la utilización de las tecnologías de la información y la comunicación (TICs), de forma tal que su análisis y valoración demande de conocimientos específicos que hagan aconsejable su especialización.*

En el ámbito de la Unión Europea, la estrategia de Ciberseguridad usa el término ciberdelincuencia, que abarca una amplia gama de actividades delictivas en las que los ordenadores y los sistemas de información se utilizan como principales herramientas para delinquir o son objeto principal del delito. La ciberdelincuencia comprende delitos tradicionales (por ejemplo, fraude, falsificación o usurpación de identidad), delitos relacionados con los contenidos (por ejemplo, distribución en línea de pornografía infantil o incitación al odio racial) y delitos exclusivamente relacionados con los

-Delitos contra la propiedad intelectual de los artículos 270 y ss del Código Penal cuando se cometan utilizando las TICs.

2. C) Delitos en los que la actividad criminal, además de servirse para su ejecución de las ventajas que ofrecen las TICs, entraña especial complejidad en su investigación que demanda conocimientos específicos en la materia.

-Delitos de falsificación documental de los artículos 390 y ss del Código Penal cuando para la ejecución del delito se hubieran empleado las TICs siempre que dicha circunstancia fuera determinante en la actividad delictiva y generara especial complejidad técnica en la investigación criminal.

-Delitos de injurias y calumnias contra funcionario público, autoridad o agente de la misma previstos y penados en los artículos 211 y ss del Código Penal cometidos a través de las TICs siempre que dicha circunstancia fuera determinante en la actividad delictiva y generara especial complejidad en la investigación criminal.

-Delitos de amenazas y coacciones previstos y penados en los artículos 169 y ss del Código Penal cometidos a través de las TICs siempre que dicha circunstancia fuera determinante en la actividad delictiva y generara especial complejidad en la investigación criminal.

-Delitos contra la integridad moral previstos y penados en el artículo 173.1 del Código Penal cometidos a través de las TICs siempre que dicha circunstancia fuera determinante en la actividad delictiva y generara especial complejidad en la investigación criminal.

-Delitos de apología o incitación a la discriminación, el odio y la violencia o de negación o justificación de los delitos de genocidio previstos y penados en los artículos 510 y 607.2 del Código Penal cometidos a través de las TICs siempre que dicha circunstancia fuera determinante en la actividad delictiva y generara especial complejidad en la investigación criminal.

-Cualquier otro tipo delictivo en cuya ejecución haya sido determinante la utilización de las TICs y en los que dicha circunstancia genere una especial complejidad en la investigación criminal.

[95] Instrucción de la Fiscalía General del Estado, *Instrucción 2/2011, del Fiscal de Sala de criminalidad informática y las secciones de criminalidad informática de las Fiscalías"* pág. 6.

ordenadores y sistemas de información (por ejemplo, ataques contra los sistemas de información, denegación de servicio o programas maliciosos)[96].

2.3 Clasificación normativa.

La tipología de internet como objeto, instrumento o el medio se refleja en el Convenio sobre la Ciberdelincuencia de Budapest, de 23 de noviembre de 2001[97], que es una de las categorizaciones más útiles de la ciberdelincuencia utilizada hoy en día, al ser una las herramienta fundamental del Derecho Internacional para la homogenización de las legislaciones penales respecto a los ciberdelitos.

El Convenio de Budapest ofrece un concepto basado tanto en la utilización de determinadas técnicas y modo de proceder informáticos (acceso ilícito a un sistema informático, interceptación ilícita, interferencias en el sistema, abuso de dispositivos, fraude informático), como en ciertos contenidos cuya vulneración se ve facilitada por el medio internet (delitos de pornografía infantil, contra la propiedad intelectual e

[96] Definición recogida en la Comunicación conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones de 7 de febrero de 2013. Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro". Y distingue o se preocupan fundamentalmente de tres grupos:
1) Delitos exclusivamente relacionados con los ordenadores y sistemas de información, en particular los ataques contra los sistemas de información:
- Acceso ilegal a un sistema de información
- Interferencia ilegal en los sistemas de información
- Interferencia ilegal en los datos
- Interceptación ilegal de datos informáticos
- Abuso de los dispositivos: producción, distribución, obtención para su utilización, importación u otra forma de puesta a disposición o posesión de dispositivos para el uso indebido de los sistemas informáticos.

2) Delitos relacionados con el contenido, en particular los relacionados con el abuso sexual de menores en línea y con la pornografía infantil:
- La producción, distribución o posesión de pornografía infantil por medio de sistemas informáticos
- La captación de menores con fines sexuales por medio de sistemas informáticos.

3) Delitos en los que los ordenadores o sistemas y tecnologías de la información fueron herramientas para delinquir u objeto principal del delito, en particular el fraude en línea y con tarjetas de pago:
- Fraude o falsificación relacionados con sistemas informáticos
- Delitos de usurpación de la identidad relacionados con sistemas informáticos
- Envío o control de los envíos de correo electrónico no solicitado

[97] El texto completo del Convenio se puede encontrar en: http://www.coe.int/t/dghl/standardsetting/t-cy/ets_185_spanish.pdf.

industrial, revelación de datos personales ...)[98]. Así, señala cuales son las conductas que entiende deben ser tipificadas en los ordenamientos penales de los países firmantes, haciendo una clasificación en tres categorías:

1. Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos. Engloba las conductas de acceso ilícito art. 2 CSC (hacking), intercepción ilícita art. 3 CSC, la interferencia de datos art. 4 CSC (por ejemplo, virus), interferencia de sistema art. 5 CSC (por ejemplo, ataques, denegación de servicio), y el uso indebido de dispositivos art.6 CSC (por ejemplo, la posesión de hackers software).

2. Delitos relacionados con la informática; estos incluyen la falsificación informática (art. 7 CSC) y el fraude informático (art. 8 CSC).

3. Delitos relacionados con el contenido[99] (la pornografía infantil, art.9 CSC y la propiedad intelectual, art. 10 CSC).

En esta clasificación destaca sobremanera el nivel de detalle y la inclusión de nuevas acciones. Aparece por primera vez como acción merecedora de reproche penal aquella relacionada con el abuso de dispositivos, que además sufre una notoria restructuración y un mayor nivel de detalle en su definición. La aplicación deja de ser una mera recomendación, como en el caso de la lista de la OCDE o el Manual de la ONU, o una declaración de intenciones como la Comunicación de la Unión Europea, para convertirse en una norma imperativa de Derecho Internacional para aquellos países que ratifiquen el Convenio.

Pero esta clasificación no es totalmente coherente, ya que no se basa en un sólo criterio para diferenciar las categorías. Tres de las categorías se refieren al objeto de la

[98] DE URBANO CASTRILLO, E. "Los delitos informáticos tras la reforma del CP de 2010 (…)". ob. cit. pág. 2.

[99] El racismo se incluye en un protocolo independiente de la Convención. Abierto a la firma el 28 de enero de 2003, entró en vigor el 1 de marzo de 2006.

protección jurídica (delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos; delitos relacionados con el contenido; y delitos relacionados con el derecho de autor), mientras que la cuarta (delitos relacionados con la informática) no se refiere al objeto de la protección jurídica sino al método. Esta incoherencia genera cierta coincidencia entre las categorías. Por otra parte, algunos términos que se utilizan para describir actos criminales ("ciberterrorismo" o "peska" "phishing") quedan comprendidos por varias categorías. No obstante, las categorías descritas en el Convenio de Budapest resultan útiles para debatir acerca del fenómeno de la ciberdelincuencia[100].

- Ciberdelitos conforme al Código Penal de 1995.

En el Código penal español no existe un título dedicado a los diferentes tipos de ciberdelitos, sino que se encuentran diseminados en diferentes títulos y artículos en los que podemos encontrar acciones típicas que, de una manera amplia, pueden llegar a ser relacionadas con la ciberdelincuencia[101].

El fenómeno del uso de la red para la práctica de actividades criminales ha de ser considerado como una actividad transversal de modo que muchos de los tipos delictivos descritos en el Código Penal no son *strictu sensu* considerados ciberdelitos si

[100] GERKE MARCO. Comprensión del ciberdelito: fenómenos, dificultades y respuesta jurídica". Sector de Desarrollo de las Telecomunicaciones de la UIT. Ginebra (Suiza) Septiembre de 2012 en: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

[101] La Fiscalía de la Comunidad Autónoma de Castilla-La Mancha en la Memoria 2014 (ejercicio 2013) pág. 191, argumenta que, partiendo del hecho incontestable de que prácticamente cualquier conducta delictiva imaginable puede ejecutarse por medios informáticos, aquéllas que mejor se adaptan al perfil de los delitos informáticos son, sin pretensión alguna de exhaustividad y relacionadas por el orden en que aparecen recogidas en el Código Penal, los delitos de amenazas, exhibicionismo y provocación sexual, relativos a la prostitución y corrupción de menores, descubrimiento y revelación de secretos, calumnia e injurias, estafa, defraudaciones de fluido eléctrico y análogas, daños, relativos a la propiedad intelectual y a la propiedad industrial, relativos al mercado y a los consumidores, receptación y conductas afines, falsedades documentales, y apología del racismo y la xenofobia.
Así las cosas, resulta evidente que no es tarea sencilla la de cuantificar los delitos informáticos que se cometen en cada territorio supuesto que, en puridad, más que de delitos informáticos debería hablarse de delitos cometidos por medios informáticos, poniendo así el acento en el medio empleado para la comisión de la infracción penal, que, como se acaba de ver, puede atentar contra los más variados bienes jurídicos, circunstancia que dificulta la correcta identificación de dichos ilícitos, que en ocasiones son registrados en función de la naturaleza de la infracción (contra la libertad sexual, contra la intimidad o contra el patrimonio, por citar algunos ejemplos) o, más frecuentemente, por la del concreto tipo penal aplicable (pornografía infantil, descubrimiento y revelación de secretos o estafa, por continuar con los ejemplos propuestos) y que explica la ausencia de datos estadísticos fiables al respecto. Existe, en todo caso, la certeza de que el aumento de este tipo de delitos es tan inexorable como el desarrollo de la tecnología de que se sirven sus autores para cometerlos.

bien la red puede ser considerada como un instrumento para la realización de tales ilícitos; así, se han descrito casos de uso de la red para la comisión de delitos de terrorismo, chantaje y extorsión; muchos otros pueden cometerse también mediante el auxilio de la red si bien no es habitual (tráfico de seres humanos, tráfico de drogas u otros delitos de tráfico). En otros el uso de la red es habitual, tal es el caso de determinados delitos de estafa (fraude) en supuestos como las cartas nigerianas[102] o los *"boiler rooms*" o falsificación de medios de pago. Finalmente, se encuentran los ciberdelitos propiamente dichos o considerados como delitos de alta tecnología, en particular los ataques contra los sistemas de información o descubrimiento y revelación de secretos.

Veamos, por tanto, qué delitos de los tipificados en el Código Penal, tras las sucesivas modificaciones desde su aprobación en el año 1995, de una forma u otra están vinculados a la informática. Aquéllos que mejor se adaptan al perfil de los ciberdelitos, relacionados por el orden en que aparecen recogidos en el Código Penal, son:

Delitos contra la libertad:

Amenazas y coacciones informáticas, artículos 169, 172 y 172 ter CP.

Delitos contra la libertad e indemnidad sexual:

- El denominado "*gromming*" o captación de menores con fines sexuales por medio de sistemas informáticos, se tipifica en el artículo 183 ter CP destinado a sancionar al que a través de medios tecnológicos contacte con un menor de dieciséis años para tener un encuentro, realice actos dirigidos a embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas.
- La producción, distribución o posesión de pornografía infantil por medio de sistemas informáticos en el artículo 189 CP.

[102] Las llamadas "cartas nigerianas" consisten en una inesperada comunicación a través de e-mails en las que el remitente promete negocios muy rentables como una fortuna inexistente pero que se pague una suma de dinero por adelantado, como condición para acceder a la supuesta fortuna.

Delitos contra la intimidad: artículos 197 a 200 CP. Se Tipifican los ciberdelitos intrusivos por excelencia:

- Delitos de descubrimiento y revelación de secretos, artículo 197.1 CP: distingue, en sus párrafos 1 y 2 entre revelación de datos que afectan a la intimidad personal y los que afectan solo a la privacidad. Introduce la conducta delictiva de aquel que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, difunde, revela o cede a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los párrafos 1 y 2. La figura del "*sexting",* se regula por primera vez en ordenamiento español en el artículo 197.7 CP que tipifica los supuestos en que las imágenes o grabaciones de otra persona se obtienen con su consentimiento pero luego se divulgan contra su voluntad, cuando la imagen o grabación se haya producido en un ámbito personal y su difusión se realice sin autorización de la persona afectada menoscabando gravemente su intimidad personal.
- El tipo de "acceso ilegal a los sistemas de información" que recoge el artículo 3 de la Directiva 2013/40/UE se incorporó al Derecho nacional en el artículo 197.1 bis.
- Interceptación ilegal de datos informáticos, se refiere el apartado 2 del artículo 197 bis.
- Abuso de los dispositivos: producción, distribución, obtención para su utilización, importación u otra forma de puesta a disposición o posesión de dispositivos para el uso indebido de los sistemas informáticos, se tipifica en el artículo 197 ter del Código Penal.

Delitos contra el honor:

- Injurias y calumnias informáticas, artículos 205 a 216 CP, el art. 211 CP se entienden con "publicidad" a las que se cometen a través de internet.

Delitos contra la propiedad y el orden socioeconómico:

- Robo inutilizando sistemas de guardia criptográfica, artículo. 238.5 CP. El artículo 239 que consideran llaves *cualquier otro instrumento tecnológico de eficacia similar.*
- Estafa informática, o el Fraude o falsificación relacionados con sistemas informáticos en el artículo 248.2 CP.
- Defraudación de telecomunicaciones informáticas, artículo 255 CP.
- Hurto de tiempo informático, o uso no autorizado de terminales informáticos, artículo 256 CP.
- Dentro de los daños informáticos, distinguimos: entre el tipo de "*Interferencia ilegal en los datos"*, a que se refiere el artículo 5 de la Directiva 2013/40/UE, que se recoge en el artículo 264 CP, el tipo de "*Interferencia ilegal en los sistemas de información"*, a que se refiere el artículo 4 de la Directiva 2013/40/UE que se incorporó al Derecho nacional en el artículo 264 bis CP y por último, lo recogido en el artículo 7 de la Directiva 2013/40/UE, en relación a los "instrumentos utilizados para cometer las infracciones", la conducta se incorporó al Derecho Penal español en el artículo 264 ter CP. Respecto a los delitos de usurpación de la identidad relacionados con sistemas informáticos, en el ordenamiento jurídico penal español no está tipificado como delito autónomo la usurpación de identidad en la red pero sí como agravante en el artículo 264.3 CP (Interferencia ilegal en los datos), y en el artículo 264 bis, apartado 3 del CP (Interferencia ilegal en los sistemas de información).
- En relación a la propiedad intelectual el artículo 270.2 tipifica el acceso o la localización en internet de obras o prestaciones objeto de propiedad intelectual incluidas las páginas de enlaces.
- Contra la propiedad industrial, arts. 273 a 275 CP.
- Espionaje informático de secretos de empresa, arts. 278 a 280 CP
- Publicidad engañosa, art. 282 CP.
- Manipulaciones en aparatos en perjuicio del consumidor, art. 283 CP
- Contra el mercado informático, art. 286 CP.
- Blanqueo informático de capitales, art. 301 CP

De las Falsedades:

- Falsedad documental, cuando el soporte sea de naturaleza informática (art. 26 CP) en el art. 390 CP.
- Usurpación de funciones públicas mediante correo electrónico, art. 402 CP.

Delitos contra la administración Pública:

- Cesión inconsentida de datos ajenos, a través de la infidelidad en la custodia de documentos y violación de secretos para su venta, hecha por empleado público, que la tiene funcionalmente prohibida, arts. 417, 418 y 423 CP.

Delitos contra la Constitución:

- En relación al ejercicio de los derechos fundamentales y libertades públicas el artículo 510 introduce lo delitos de odio a través de medios de comunicación social, internet o uso de las tecnologías de la información[103].

Delitos de terrorismo:

La regulación de los delitos de terrorismo en el Código Penal fue modificada por la LO 2/2015, de 30 de marzo. Así, el artículo 573 CP enumera los delitos que son considerados de terrorismo, y específicamente en su apartado 2º, se refiere como delitos terroristas a "*los delitos informáticos tipificados en los artículos 197 bis y 197 ter y 264 a 264 quater cuando los hechos se cometan con alguna de las finalidades a las que se refiere el apartado anterior.*"

Estas finalidades son:

"1.a Subvertir el orden constitucional, o suprimir o desestabilizar gravemente el funcionamiento de las instituciones políticas o de las estructuras económicas o sociales

[103] España ratificó (BOE 20 de enero de 2015) el Protocolo adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos, hecho en Estrasburgo el 28 de enero de 2003. Se contempla como un supuesto de agravante específica respecto de los tipos penales de Delitos cometidos con ocasión del ejercicio de los derechos fundamentales y de las libertades públicas garantizados por la Constitución, cuando los hechos se hubieran llevado a cabo a través de un medio de comunicación social, por medio de internet o mediante el uso de tecnologías de la información, de modo que, aquel se hiciera accesible a un elevado número de personas. La sanción caso de concurrir esta agravante será el de las penas previstas en los apartados anteriores en su mitad superior (artículo 510.3º del CP).

del Estado, u obligar a los poderes públicos a realizar un acto o a abstenerse de hacerlo.

2.a Alterar gravemente la paz pública.

3.a Desestabilizar gravemente el funcionamiento de una organización internacional.

4.a Provocar un estado de terror en la población o en una parte de ella".

La sanción de estos delitos viene establecida en el artículo 573 bis.3 CP "se castigarán con la pena superior en grado a la respectivamente prevista en los correspondientes artículos."

Por otro lado, también se tipifica la conducta de "*auto adiestramiento*" mediante el acceso habitual a servicios de comunicación. El artículo 575 tipifica el adoctrinamiento y el adiestramiento militar o de combate o en el manejo de toda clase de armas y explosivos, incluyendo expresamente el adoctrinamiento y adiestramiento pasivo, con especial mención al que se realiza a través de internet o de servicios de comunicación accesibles al público, que exige, para ser considerado delito, una nota de habitualidad y un elemento finalista que no es otro que estar dirigido a incorporarse a una organización terrorista, colaborar con ella o perseguir sus fines.

También se regula en el CP la difusión de servicios o contenidos accesibles al público a través de los medios de comunicación, internet o por medio de servicios de comunicaciones electrónicas o mediante el uso de tecnologías de la información de mensajes que enaltezcan o justifiquen alguno de los delitos de terrorismo o de quienes hayan participado en su ejecución o realización de actos que supongan descrédito, menosprecio o humillación de las víctimas de los delitos terroristas o de sus familiares (art. 578.1º y 2º CP).

Asimismo se prevé la retirada de los contenidos ilícitos de la red (art. 578.4 CP).

Por último, también se castiga la incitación, provocación, conspiración y proposición, públicamente, para cometer delitos de terrorismo a través de cualquier medio, incluidas las tecnologías de la información y la comunicación (art. 579 CP).

De los delitos de traición y contra la paz o la independencia del Estado y relativos a la Defensa Nacional:

- Descubrimiento y revelación de secretos relativos a la defensa nacional, artículos 598 y 603 CP.

3. TÉCNICAS DE COMISIÓN DE LOS CIBERDELITOS.

En la medida en que en este trabajo contiene necesariamente conceptos informáticos, se hace necesario concretar, siquiera sea de manera elemental, el sentido de los mismos. Es importante analizar las diversas técnicas usadas por los ciberdelincuentes para afrontar el estudio de su investigación y prueba.

Estas técnicas están en constante desarrollo, por lo que es muy difícil adelantarse y hacer una enumeración exhaustiva, ya que depende no solo de los ciberdelincuentes y de las TIC sino también de los desarrollos en el campo de la seguridad.[104] Por ello, estimo preferible describir las técnicas más usadas por la ciberdelincuencia[105].

En primer lugar hay que hacer referencia al término "*HACKING"*, que en relación con la tecnología data de 1960[106]. "Hacking", anglicismo con el que se alude al

[104] LEUKFELDT R & DE JONG, E. *Basic Cybercriminal Techniques & Techniques to cause damage*. En "Cyber Safety: An Introduction" (…) ob. cit. pág. 167.

[105] MORÓN LERMA, E. "Internet y Derecho Penal: Hacking y otras Conductas Ilícitas en la Red". ob. cit. pág. 80.

[106] LEUKFELDT R & DE JONG, E. *Hacking.* En "Cyber Safety: An Introduction" (…) ob. cit. págs. 103. FURNELL, STEVEN. "Cybercrime. Vandalizing the information society". Addison-Wesley, A Pearson Education Limited, Great Britain 2002. págs. 8 y ss. FURNELL, STEVEN. *Hackers, viruses and malicious software,* en "Handbook of Internet crime". Ed. Willan publishing. Devon (UK), 2010. pág. 6.

simple acceso no autorizado a ordenadores y sistemas informáticos ajenos, utilizando las redes públicas de telefonía o transmisión de datos y con propósitos distintos al de causación de daños. El nombre *hacker*, neologismo utilizado para referirse a un experto (Gurú) en varias o alguna rama técnica relacionada con las tecnologías de la información y las telecomunicaciones: programación, redes, sistemas operativos[107].

Tradicionalmente en la doctrina se distingue entre el hacking y cracking; así, el Cracker (criminal hacker, 1985) es alguien que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño a su objetivo. El hacker, tradicionalmente era el término usado para quién entraba en los sistemas informáticos con buenas intenciones (ejemplo, demostrar agujeros en la seguridad de las redes) mientras que el término cracker era el usado para quién desempeñaba las mismas actividades pero con malas intenciones, con la destrucción como objetivo. Sin embargo, hoy día se impone el uso más generalizado del primero.

Los ataques que los hackers pueden realizar a un ordenador son variadísimos. Como técnicas básicas para ejecutar otros ataques, hay que citar de una parte a la llamada ingeniería social; que consiste en persuadir a los usuarios de hacer algo que normalmente no haría, como dar una contraseña u otra información personal (por ejemplo, haciéndose pasar por un empleado de una compañía que consigue la contraseña de un usuario diciéndole que se está probando un nuevo sistema). Y de otra a las técnicas escudo; como pueden ser las técnicas de anonimización para evitar descubrir la IP desde la que operan o los encriptados.

---

[107] GONZÁLEZ RUS J.J. *Los ilícitos en la red (I): hackers, crakers cyberpunks, sniffers, denegación de servicios y otros comportamientos semejantes*. En "El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales" (Romeo Casabona, coord.). Ed. Comares, Granada, 2006, pág. 241. "*el término hacker viene del inglés hack, que se usa normalmente en el contexto de los leñadores, en el sentido de cortar algo en pedazos o en el de dar puntapiés. En el mundo informático se usa para referisrse a alguien que conoce los sistemas operativos con gran profundidad, hasta el punto de poder decir que lo había cortado en pedazos".*

Las últimas modalidades comisivas se han diversificado tanto que es necesario precisar algunos de los conceptos de la nueva terminología informática referida al modo en que puede producirse los posibles ataques informático[108].

Así, se habla de *SOFTWARE* MALICIOSO O *MALWARE* para describir un conjunto de códigos y programas que introducidos en un sistema informático, originan problemas de utilización u operatividad del mismo, de sus programas de funcionamiento o alteración o borrado de datos[109].

Existen muchas clases de *malware* y se propagan de distintas formas: algunas veces vienen dentro de un programa que se instala, en otros casos utilizan alguna vulnerabilidad en el sistema operativo o el navegador, pero usualmente son instalados por alguna acción del usuario (como hacer clic en un archivo adjunto de correo o descargar algo en internet).

Como tipos de *malware* se pueden enumerar los siguientes[110]:

1. Virus: este término se usa de forma genérica para referirse a un software malicioso que trata de hacer estragos en el ordenador. Sin embargo, la palabra correcta es *malware*. El virus es un programa informático diseñado específicamente para reproducirse y evitar su detección. Realizan básicamente dos funciones: replicarse de un sistema informático a otro y situarse en los ordenadores de forma que pueden destruir o modificar programas y ficheros de datos, presentar un determinado mensaje, provocar fallos en el sistema operativo o interferir los procesos normales del sistema operativo. El virus se reproduce copiándose en el disco duro, en programas informáticos o a través de redes informáticas. (Un ejemplo de virus informático fue el *viernes 13 o Jerusalén,* creado en Israel en el año 1988, que cada viernes 13 borraba todos los programas que se ejecutaban en el ordenador).

---

[108] DE LA MATA BARRANCO, NORBERTO J Y HERNÁNDEZ DÍAZ, LEYRE, "El delito de daños informáticos: una tipificación defectuosa". Estudios Penales y Criminológicos, vol. XXIX (2009). pág. 313.

[109] Los virus, gusanos, troyanos y demás son *malware*. Esta palabra es una versión corta para designar código malicioso o un software malicioso.Todos estos programas están diseñados para hacer daño, robar o infligir acciones ilegitimas en ordenadores individuales o redes completas.

[110] GONZÁLEZ RUS J.J. Los ilícitos en la red (I): hackers, crakers cyberpunks, sniffers (…) ob. cit. pág. 265.

2. **Gusano:** este programa también se reproduce a si mismo pero suelen correr en el fondo del sistema como un programa propio. Se esparce rápidamente porque aprovecha las vulnerabilidades del sistema, y a veces es difícil de detectar porque se vale de métodos de transporte de información que el sistema operativo tiene integrado[111]. Un gusano es un virus informático que tiene la propiedad de duplicarse a sí mismo, aunque a diferencia de un virus, un gusano no precisa alterar los archivos de programas. Los gusanos siempre dañan la red, mientras que los virus infectan o corrompen los archivos del ordenador que atacan. (Un ejemplo de gusano informático fue *I LOVE YOU* que en mayo del año 2000 infectó más de 50 millones de ordenadores, entre ellos los equipos informáticos del Parlamento Británico).

3. Troyano: los troyanos se disfrazan de software con buenos propósitos, pero terminan comportándose de forma maliciosa, pues son programas hechos para engañar al usuario y hacer daño al sistema. Los troyanos pueden hacer cosas como robar datos, borrar archivos y hasta instalar otros tipos de *malware* (como ejemplo de software dañino del tipo *troyano* muy avanzado hay que destacar por su importancia el Stuxnet[112]). Un nuevo tipo de troyano es el denominado *Backdoor* (puerta trasera) que

[111] Se transmiten fundamentalmente por el correo electrónico y se auto ejecutan sin necesidad de que el receptor realice acción alguna para ello. Para que se produzca el contagio basta con tener activada la vista previa en la carpeta de entrada del correo, instalándose el gusano en el ordenador de la víctima. Su particularidad es que al ejecutarse en una máquina exploran automáticamente la red a la que está conectado el ordenador infectado para buscar vías de penetración en las misma, acabando de esa forma de colapsar redes locales o servidores. GUSANO TROYANO: se difunden como fichero anexo a los gusanos y que al activarse permite tener acceso remoto de la máquina infectada.

[112] JOYANES AGUILAR, L. Introducción: Estado del Arte de la Ciberseguridad. En "Ciberseguridad. Retos y amenazas a la Seguridad Nacional en el Ciberespacio". Instituto Español de Estudios Estratégicos. Instituto Universitario "General Gutiérrez-Mellado". Ministerio de Defensa, Cuaderno de estrategia nº 149. Madrid, diciembre de 2010. pág. 27 un programa, que aprovecha la vulnerabilidad MS10-0466 de los sistemas operativos Windows CC, empleados en los sistemas SCADA (*Super- visory Control and Data Acquisition*) fabricados por Siemens y que se utiliza en infraestructuras críticas tales como el control de oleoductos, plataformas petroleras, centrales eléctricas, centrales nucleares y otras instalaciones industriales con el objetivo de sabotearlos. Se piensa que una vez dentro de una planta podría reprogramar las centrifugadoras para hacerlas fallar sin que se detectara. "***Stuxnet*** *es un troyano muy sofisticado que utiliza técnicas de rootkit para instalarse en el sistema operativo. El troyano queda camuflado y latente en el equipo infectado hasta que su autor decide activarlo. Se detectó el mes de junio de 2010 por una compañía de seguridad informática de Bielorrusia, VirusBlokAda que lo descubrió en unos ordenadores pertenecientes a un cliente en Irán. Entonces se pensó que se trataba de un programa dañino diseñado para robar procesos de fabricación o bocetos de productos; sin embargo después del ataque de septiembre se piensa que ha sido creado para sabotajes de infraestructuras críticas de las naciones. Este tipo de troyanos no van destinados a la infección masiva de ordenadores domésticos sino que está pensado para atacar a infraestructuras críticas o incluso sabotajes industriales, donde puede aumentar o disminuir el caudal de un oleoducto o dañar a una central nuclear. Dado que va dirigido contra infraestructuras críticas que no utilizan Internet, se supone que el troyano se introdujo en los ordenadores a través de lápices de memoria tipo USB y luego se multiplica a sí mismo, pasando de un*

permite a un atacante tomar el control remoto del sistema infectado para llevar a cabo una gran diversidad de acciones: espiar el escritorio remoto, realizar capturas de pantalla o de la *webcam*, subir o descargar archivos, alterar el funcionamiento normal del sistema, etc.

4. Adware: para infectar un sistema operativo el Adware usualmente se instala junto a otro software que lo introduce en su instalador, y generalmente se puede eliminar si se desinstala el programa. El adware sirve para entregar publicidad de forma invasiva y en la mayoría de los casos se utiliza para conseguir más información de la que el usuario quiere dar. Por eso su nombre en inglés comienza con la palabra "*ad*", que significa "anuncio". (Algunos ejemplos de programas que incluyen adware pueden ser Alexa, MyWebSearch, FlashGet etc…)

5. Spyware (programas espías)**:** este software monitorea el ordenador donde está instalado y recolecta información para su creador. Puede no ser una gran amenaza para el usuario (como por ejemplo cuando visitamos una página web y toman información para hacer la navegación más eficiente al regresar a ella), pero en algunos casos puede ser muy dañino e invasivo, monitoreando hasta lo escrito con el teclado o el propio movimiento del *mouse*. (Ejemplos de spywares son software de registro de clave o de capturas de pantalla del ordenador de la víctima. Se consideran una de las formas más peligrosas de malware como su objetivo no es otro que invadir la privacidad)[113].

6. Sniffers (o rastreadores)**:** son programas que permiten introducirse en el disco duro de los ordenadores conectados a la red, buscando un cierto tipo de información[114].

7. Bombas Lógicas: son rutinas o alteraciones de programas que producen cambios o borrados de ficheros o perturbaciones del sistema en un momento posterior a aquel en el que se introducen, activándose cuando se cumple una determinada condición (por ejemplo, a una determina fecha). Están ideadas para dañar el sistema o los datos, aunque pueden utilizarse para ordenar pagos, realizar transferencias de fondos etc. (Un

---

ordenador a otro, instala programas troyanos de espionaje para recoger información y puede dañar tanto sitios web como sistemas operativos".

[113] FURNELL, STEVEN. *Hackers, viruses and malicious* (…) ob. cit. pág. 6 y ss.

[114] GONZÁLEZ RUS J.J. Los ilícitos en la red (I): hackers, crakers cyberpunks, sniffers (…) ob. cit. pág. 242.

ejemplo de bomba lógica se produjo en la empresa americana "Fannie Mae" el 17 de febrero de 2009, donde al parecer un ex ingeniero descontento despedido en octubre de 2008 atacó mediante una bomba lógica el sistema informático de la empresa, que se vio obligada a cerrar una semana para repara los daños causados).

8. Botnets[115]: los denominados robots de la red son redes de ordenadores "zombis", que se crean infectando ordenadores sin que sus propietarios lo sepan. Cada máquina reclutada por el virus se pone en contacto sigilosamente con el cibercriminal a la espera de sus órdenes. El virus puede enviarse por correo electrónico aunque lo habitual es ponerlo en páginas web, fundamentalmente que tengan muchas visitas. Una vez dentro del ordenador, el virus descargará un programa y lo instalará (es el *bot,* el lazo entre el ordenador infectado y la *net,* la red que permite su control remoto). Los botnets se usan mayoritariamente para el envío masivo de correo basura y virus, para el espionaje, sea de empresas o de la información bancaria de los dueños de los ordenadores infectados o para el fraude publicitario[116]. (Un ejemplo de malware tipo botnet es el llamado Zeus)[117].

9. Exploit: código que utiliza una vulnerabilidad del sistema o de algún punto en concreto de éste para aprovechar esta deficiencia e introducirse en un sistema sin estar autorizado. El programa que explota la vulnerabilidad no es un código malicioso en sí mismo, pero, como en el caso anterior, es la puerta de inicio al envío de códigos maliciosos posteriores que representen amenazas reales para el sistema. También son utilizados para simplemente obtener un acceso a un equipo no autorizado, aún sin tener como finalidad el infectarlo con algún malware posteriormente.

---

[115] JOYANES AGUILAR, L. Introducción: Estado del Arte de la Ciberseguridad (…) ob. cit. pág. 28.

[116] El fraude consiste en crear una página cualquiera, poner en ella algunos anuncios legales y hacer que todos los ordenadores de la botnet los visiten. A efectos prácticos en las estadísticas se verá que los clics provienen de cientos o miles de direcciones IP diferentes, repartidas por todo el mundo y por tanto parecerá que son usuarios legítimos y no una estafa, de esta forma el anunciante deberá pagar el porcentaje convenido.

[117] Zeus es un virus de tipo botnet (troyano) que se propaga por los navegadores, tanto Explorer como Firefox. El malware recopila información del usuario y contraseñas de internet y redes sociales, utilizándolas para suplantar la identidad y realizar robo de datos bancarios, datos de tarjetas de crédito o enviar spam. Miles de empresas de todo el mundo han caído en esta pandemia digital. Además a primeros de noviembre de 2010 se detectó que el virus Zeus había afectado a dispositivos móviles. Uno de los grandes peligros es que el ataque Zeus consiguió propagarse por las redes sociales hasta obtener 10 millones de dólares de un banco en sólo 24 horas introduciendo un malware en el ordenador personal del tesorero a través de una web infantil a la que accedió su hijo.

10. Droppers: bajo una apariencia de programa legítimo, los droppers instalan y ejecutan otros programas y archivos maliciosos en el equipo del usuario atacado. La diferencia de los droppers con los troyanos comunes es que éstos están destinados para alojar información o paquetes de datos concretos en el equipo infectado, y no suponen un fin en sí mismos, sino que son una herramienta más para conseguir un fin. Al ejecutarse un dropper, su código se carga en la memoria y posteriormente se extrae el fragmento de código malicioso que se desee almacenar de forma ilegítima en el sistema infectado y se graba en el sistema de archivos.

11. Rootkit: herramienta cuyo objetivo principal es adquirir el control de un sistema de forma ilícita y poder conseguir privilegios equiparables al administrador. Los rootkit generalmente son la herramienta utilizada por los infractores inmediatamente posterior al uso de los exploit, por lo que en el proceso de ataque a un sistema informático, primero se encontraría la debilidad del mismo y se atacaría mediante un exploit, y tras conseguir con éxito adentrarse en el sistema se comenzaría a ejecutar la herramienta rootkit con la que se podría causar el daño interno en el sistema siendo prácticamente invisible a los ojos del usuario infectado[118].

12. DDoS[119]: los ataques DDoS (Distributed Denial of Service) son una forma relativamente sencilla y efectiva de hacer caer a una Web. Las acciones se pueden realizar de forma voluntaria siguiendo las instrucciones dadas para iniciar el ataque a una hora señalada en una convocatoria mediante foros en la Red o utilizando redes de ordenadores previamente infectados por virus (*botnet*) de forma que los usuarios ni siquiera son conscientes de que participan[120].

---

[118] En el año 2005 saltó la noticia de que la empresa Sony utilizaba rootkits en algunos de sus sistemas anti copia para la play station 3, y se vio obligada a crear una aplicación para eliminar este Rootkit, por el peligro que suponía que cualquier creador del malware podía alojar alguno en dicha carpeta.

[119] JOYANES AGUILAR, L. Introducción: Estado del Arte de da Ciberseguridad (…) ob. cit. pág. 27.

[120] INDA ORTIZ DE ZÁRATE. F. J. "La investigación policial en el ámbito de la informática". Cuaderno del Instituto Vasco de Criminología. nº 20. San Sebastián, 2006. pág. 182. Los tipos más frecuentes de ataques DDos, son:
– Ataque "*Smurf*": el *hacker* satura la red con mensajes de respuesta "ping" *Internet Control Message Protocol* (ICMP). Envía solicitudes "ping" ICMP dirigidas a una dirección "*broadcast*" con la dirección fuente orientada hacia la máquina que se desea atacar. Todos los "*host*" de la red seleccionada responden con respuestas "ping" dirigidas a las máquinas objetivo, amplificando cientos de veces su mensaje original y ocultando la propia dirección real.
– Ataque TCP SYN: envía solicitudes falsas de conexión TCP (*Transmission Control Protocol*) a la máquina objetivo, sin estar completas las conexiones, desde una dirección "*spoofed*" (técnica en la que el

13. El spam: correo electrónico no solicitado o "basura", normalmente enviado de forma masiva a destinatarios en todo el mundo y que suele relacionarse con productos farmacéuticos y pornografía. Spam de correo electrónico también se utiliza para enviar correos electrónicos de phishing[121] o malware y puede ayudar a maximizar la rentabilidad potencial para los delincuentes.

Por último, es destacable también otro novedoso tipo de ataque que ha surgido en los últimos años, el de los denominados ***blended threats***, especialmente peligrosos por combinar las características de virus, gusanos y troyanos con las vulnerabilidades de internet y de sus servidores para crear, transmitir y propagar los ataques[122].

En definitiva, aunque estas técnicas son los medios más comunes para violar la integridad y funcionalidad de un sistema informático, en la actualidad no son el único método para hacerlo, ya que se han desarrollado otro tipo de técnicas para poder realizar abusos en sistemas ajenos de forma independiente de éstos o en complemento de su labor. Un resumen de las técnicas más comunes usadas por los ciberdelincuentes para llevar a cabo sus propósitos cibercriminales, sería:

- Las técnicas de anonimato (como, el uso de datos personales falsos sin posibilidad de control, uso de "Proxys" anónimos, servidores de correo Web anónimo, utilización de sistemas creadores de Web anónimas, el uso de los "cibercafés" carentes

---

atacante falsifica su dirección ocultando la identidad de su máquina). Tales solicitudes incompletas bloquean la "*request table*" del objetivo e impiden a éste aceptar cualquier otro tipo de solicitud de conexión.
– Ataque UDP: envía cantidad de mensajes UDP (*User Datagram Protocol*) al objetivo, saturando la amplitud de banda de la red de trabajo disponible.
– Ataque TCP: igual al anterior pero utilizando mensajes TCP, lo que crea la complicación de que la mayor parte del tráfico real en la red es de este tipo.
– Ataque *Distributed DoS*: replica el "*host*" atacante cientos de veces y lo distribuye por Internet. Controlados de forma remota y centralizada, la localización y cierre de una máquina permite que el resto siga activado. Para todos ellos suelen utilizarse programas como *Trinoo, TFN, Stacheldraht, TFNak* y otros.

[121] INDA ORTIZ DE ZÁRATE, F. J. "La investigación policial en el ámbito de la informática" ob. cit. págs. 179 a 195. *Phishing*: Fraude bancario realizado usurpando páginas web corporativas de bancos, o explotando sus vulnerabilidades, y que tiene como fin hacerse con datos bancarios. Ataque con la intención de robar información confidencial de un usuario. Suele hacerse a través de mensajes. Los usuarios suelen ser persuadidos para abrir algún archivo adjunto en el mensaje o para clicar una página web.
Pharming: Fraude "on-line" que consiste en suplantar el sistema de resolución de nombres de dominio -DNS- para conducir al usuario a una página web falsa.

[122] DE LA MATA BARRANCO, N. J Y HERNÁNDEZ DÍAZ, L. "El delito de daños informáticos: una tipificación defectuosa (…) ob. cit. pág. 313.

de la más mínima regulación, la conectividad a través de redes WIFI ajenas carentes de seguridad y el uso de programas de encriptación o de estenografía para ocultar contenidos).

- El uso de programas maliciosos (tipo troyano que permiten el control remoto de los equipos, el envío de virus, gusanos, spyware, adware, programas no deseados que controlan los sistemas ajenos, creando redes de equipos infectados (botnets) bajo control de delincuentes informáticos, el uso de diccionarios y robots para ataques de fuerza bruta contra sistemas de encriptación, el envío de publicidad no deseada (spam)).
- Las técnicas de ingeniería social que permiten suplantar identidades, capturar contraseñas, utilizar productos bancarios para estafar o engañar apoyado en contenidos falsos de la red.
- La explotación de "bugs" o agujeros de seguridad mediante "exploits" diseñados al efecto para facilitar el trabajo, que permiten el control de equipos ajenos.
- Las técnicas de denegación de servicios (DoS) para interrumpir la operatividad de sistemas informáticos.
- A ellos hay que añadir, la distribución contenidos delictivos como la pornografía infantil, la inserción de contenidos lesivos contra el honor o imagen o el envío de mensajes amenazantes y su conservación y mantenimiento en "paraísos informáticos" para preservarlos de cualquier control o investigación judicial.

Todo ello, constituyen un incompleto abanico de técnicas y conductas que son utilizadas por algunos usuarios de la red en interés propio y con perjuicio de terceros[123], generando conductas y situaciones que precisan ser descritas para que puedan obtener una adecuada respuesta jurídico-penal y procesal.

[123] *Vid.* Estudio sobre la cibercriminalidad en España año 2015. Ministerio del Interior. Secretaría de Estado de Seguridad. Gabinete de Coordinación y Estudios.

CAPÍTULO TERCERO

JURISDICCIÓN Y COMPETENCIA.

1. COMPETENCIA EN RELACIÓN CON LOS CIBERDELITOS COMETIDOS EN TERRITORIO ESPAÑOL Y PARCIAL O TOTALMENTE FUERA DEL TERRITORIO ESPAÑOL.

Muchos de los principales obstáculos que surgen en la investigación de los ciberdelitos derivan de su carácter transfronterizo, ya que por su propia naturaleza y características frecuentemente se desarrollan y/o producen efectos en distintos territorios, lo que puede originar problemas en la determinación de la jurisdicción y competencia aplicable al caso.

A la hora de perseguir determinados delitos cometidos por medios informáticos se plantean ciertas dudas sobre el lugar de comisión de los mismos, habida cuenta de que la acción o la comunicación delictiva se realiza desde un emplazamiento o lugar en muchas ocasiones ignorado a través de un ordenador u otro equipo con acceso a internet, que no siempre está fijo y que puede redireccionar a través de diversos servidores ubicados en lugares y países diversos, pudiendo producirse los efectos en muchos y muy diversos emplazamientos físicos. El Convenio sobre Ciberdelincuencia regula estas cuestiones en su artículo 22 sobre jurisdicción[124]

[124] Art. 22 del Convenio sobre ciberdelincuencia, dispone:
"*1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para atribuirse la competencia respecto a cualquier infracción penal establecida en los artículos 2 a 11 del presente Convenio, cuando la infracción se haya cometido:*
en su territorio;
a bordo de una nave que ondee pabellón de ese Estado;
a bordo de una aeronave matriculada en ese Estado;
por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar donde se ha cometido o si ningún Estado tiene competencia territorial sobre el mismo.
2. Las Partes podrán reservarse el derecho de no aplicar, o de aplicar sólo en ciertos casos o condiciones específicas, las reglas de competencia definidas en los párrafos 1b a 1d del presente artículo o en cualquiera de las partes de esos párrafos.

En el derecho interno Español no existen normas específicas sobre la determinación de la jurisdicción española para el conocimiento de los ciberdelitos, más allá de lo dispuesto con carácter general en el artículo 23 de la LOPJ.

El Tribunal Supremo considera que para la persecución del ciberdelito (que normalmente se comete desde un ignorado lugar y produce sus efectos en diversas ubicaciones geográfica) es competente para su persecución, el juez de todos y cada uno de los lugares donde se manifiestan sus efectos, lo que incluye tanto el lugar de la acción como el del resultado[125].

Se trata del denominado principio de ubicuidad,[126] criterio adoptado a partir del Acuerdo no jurisdiccional del Pleno del Tribunal Supremo de 3 de febrero de 2005, según el cual: "*el delito se comete en todas las jurisdicciones en las que se haya realizado algún elemento del tipo. En consecuencia, el Juez de cualquiera de ellas que primero haya iniciado las actuaciones procesales, será en principio competente para la instrucción de la causa".*

Esta regla se establece de forma inicial, toda vez que si, conforme vaya avanzando la investigación de la causa llegara a determinarse el lugar geográfico

---

3. Las Partes adoptarán las medidas que se estimen necesarias para atribuirse la competencia respecto de cualquier infracción mencionada en el artículo 24, párrafo 1 del presente Convenio, cuando el presunto autor de la misma se halle en su territorio y no pueda ser extraditado a otro Estado por razón de la nacionalidad, después de una demanda de extradición.
4. El presente Convenio no excluye ninguna competencia penal ejercida por un Estado conforme a su derecho interno.
5. Cuando varios Estados reivindiquen su competencia respecto a una infracción descrita en el presente Convenio, los Estados implicados se reunirán, cuando ello sea oportuno, a fin de decidir cuál de ellos está en mejores condiciones para ejercer la acción penal."

[125] MARCHENA GÓMEZ, M. "Dimensión jurídico-penal del correo electrónico", en Diario La Ley nº 6475, Sección Doctrina, 4 de mayo de 2006. pág. 14 "*La teoría de la ubicuidad, por ejemplo, permitirá entender que la inoculación de un potente virus destructivo mediante el correo electrónico, llevada a cabo desde fuera de España por un no nacional, pero que expande sus nocivos efectos en sistemas informáticos radicados en territorio español, puede ser perseguida en nuestro país, en la medida en que el delito, atendiendo al resultado, también puede reputarse cometido en España. Esa conclusión estaría vedada si entendiéramos aplicable la teoría de la actividad, pues el delito, en la medida en que la acción se habría desarrollado por un extranjero, fuera de nuestro territorio y el delito de daños no se halla en el catálogo de figuras delictivas del art. 23 de la LOPJ, no se entendería cometido en los límites jurisdiccionales españoles".*

[126] Actualmente, no se plantean en la doctrina discrepancias respecto del principio de ubicuidad incluido en este Acuerdo del Pleno no Jurisdiccional del Tribunal Supremo de 3 de febrero de 2005.

concreto desde el que se introdujeron los datos delictivos en la red[127], se produjo el daño, se destruyó el sistema operativo o se contaminaron los archivos[128]cabe la inhibición a favor del Juez así determinado, conforme a la regla general del *forum delicti comisi* del art. 14 de la LECrim[129].

En la práctica de los Tribunales, cuando los efectos se manifiestan en distintos territorios del país, normalmente se procede a la apertura de tantas investigaciones como lugares se vean afectados, bien porque en ellos se ha materializado alguna de las fases de ejecución de la actividad delictiva, bien porque constituyen el lugar de residencia de los perjudicados por la misma. Ante esta situación resulta esencial llevar a cabo una

[127] ATS 16 de marzo de 2016 (cuestión de competencia 20040/2016) en un asunto sobre tenencia y distribución de material pornográfico infantil a través de internet, resolvió la competencia a favor del juzgado del lugar en el que se hayan introducido en la red los contenidos delictivos. *"La determinación de lugar de comisión del delito en el caso de difusión y tenencia de material pornográfico no se hará con base en la teoría de la ubicuidad o la del resultado sino con base en la teoría de la actividad, y ello porque en este tipo de delitos existe gran dificultad para determinar con precisión el lugar de difusión del contenido pornográfico. De esta forma, decíamos en el ATS de 21/03/2014, con cita de otros, que en los delitos cometidos a través de internet serán competentes los Juzgados del lugar en el que se hayan introducido en la red los contenidos delictivos. Asimismo de conformidad con esta misma Jurisprudencia, cada persona que distribuye, ofreciendo desde su ordenador la descarga de archivos de pornografía infantil, comete un delito, sin que la mera conexión informática, decíamos en el ATS de 10/09/2015, suponga la existencia de conexión delictiva, por lo que deben seguirse procedimientos distintos, correspondiendo la competencia a los Juzgados de los lugares en los que cada imputado haya desplegado su comportamiento".*

[128] Con base al principio de ubicuidad, respecto del delito de injurias cometido en un foro de internet se planteó una cuestión negativa de competencia entre los Juzgados del domicilio del denunciante y aquél en que radicaba el servidor de la página web, el Auto del Tribunal Supremo de 12 de enero de 2012 (Rec. 20591/11) atribuyó la competencia al Juzgado en el que se habían iniciado las actuaciones, lugar del domicilio del denunciante y ofendido y lugar donde se reciben las ofensas. Dicha resolución vino a establecer expresamente que: "*... el criterio de que en los delitos cometidos a través de internet serán competentes los juzgados en los que se haya introducido en la red los contenidos delictivos, se refiere a los delitos de pornografía infantil, pero siempre ha sido matizada cuando nos encontramos con delitos de diferente naturaleza como en el caso que nos ocupa de las injurias ya sea vía internet o telefónica, al igual que en el caso de los daños informáticos, delito de resultado que no se comete desde donde se lanza el ataque sino donde se produce los daños, se destruye el sistema operativo o se contaminan los archivos...).*

[129] Auto del Tribunal Supremo de 5 de octubre de 2011 (rec. 20137/2011) en un ataque hacker a páginas web, determinó la competencia del lugar donde se comenzó a realizar actuaciones, aunque los ordenadores desde los que se cometieron estuvieran en otro lugar. "*nos encontramos ante una acción conjunta realizada por expertos hackers y de común acuerdo, y un ataque planificado y organizado desde diferentes IP a múltiples páginas web, de manera que de acuerdo con el Art. 14 y 18 Ley de Enjuiciamiento Criminal el juzgado competente es donde se cometió el delito denunciado y primero comenzó a conocer de las actuaciones que además coincide con el domicilio de los perjudicados. Si tenemos en cuenta el criterio de la mayor facilidad y conveniencia en la investigación también utilizado por nuestra jurisprudencia que en este tipo de delitos es mantenido por el Convenio sobre el Cibercrimen, suscrito en Budapest el 23 de noviembre de 2001, ratificado por España, que determina que será competente el Estado "que esté en mejores condiciones para ejercer la persecución del delito" (art. 22.5).*

labor de coordinación[130] de todas las investigaciones a fin de evitar las indeseadas dilaciones provocadas por recíprocas inhibiciones entre los órganos judiciales, con el consiguiente riesgo de pérdida o inutilización de las evidencias informáticas, y al tiempo dar una respuesta penal global y adecuada a la verdadera entidad del delito.

En este sentido, se plantea además la cuestión de quién será el juez competente para la adopción de las diligencias de investigación oportunas. Conforme al principio de ubicuidad, lo será aquél en cuyo territorio haya indicios de que se están llevando a cabo actos típicos de la comisión del delito investigado[131]. En cualquier caso, la solución pasa por considerar que se trata de una medida que debe adoptarse (autorizarse o no) por el Juez al que se le solicite (si hay indicios de comisión del tipo del delito en su territorio), sin perjuicio de que de si él no se considerase competente, lleve a cabo, conforme a lo establecido en la LECrim, los trámites para proceder a la inhibición al Juzgado que estime competente, conservando no obstante su competencia hasta que una resolución definitiva la fije, por lo que dado el plazo de tiempo en que tardan en resolverse estas cuestiones, parece que deberá pronunciarse sobre la autorización solicitada y comenzar la investigación (o instrucción)[132].

No se consideraría adecuado denegar la autorización por falta de competencia, ya que, como se han encargado de recordar nuestros Tribunales, cualquier actuación del

[130] Debe destacarse que uno de los objetivos prioritarios de la Fiscalía contra la criminalidad informática se centra específicamente hacer posible la necesaria coordinación de las investigaciones incoadas con ocasión de los múltiples efectos que una misma actividad ilícita puede generar en distintos puntos del territorio nacional, labor que se está llevando a efecto desde su constitución en el año 2011, contando con la ventaja de que la propia organización interna de la fiscalía permite articular coherentemente la adecuada respuesta a éste fenómeno mediante un sistema fluido y permanente de comunicación interna entre los Fiscales delegados de la especialidad en cada una de las provincias españolas.

[131] Pero, ¿qué sucederá cuando los indicios se manifiesten en diversos territorios? ¿Podrá elegirse el que se considere más adecuado por la Policía Judicial? Y en el caso de que cambien los efectos de la acción delictiva, ¿debería cederse la competencia a favor del Juez del territorio donde se esté desarrollando en ese momento la acción delictiva o por el contrario, al haber autorizado una medida limitativa de derechos, el primer juez que autorizó tendrá que asumir la instrucción de la causa, cualesquiera que sean luego los lugares en que se extienda el desarrollo principal de la actividad delictiva y aunque en el suyo ya no se produzca ninguna otra actividad?

[132] VILLAGÓMEZ MUÑOZ, A. "Otras medidas de investigación limitativas de derechos reconocidos por el art. 18 C.E. referencia concreta a los dispositivos de seguimiento y localización". Ponencia presentada en el curso de formación continua de Fiscales del año 2016, sobre La interceptación de las comunicaciones telefónicas y telemáticas, celebrada en Madrid del 27/4/2016 al 29/04/2016. www.cej.mjusticia.es pág. 12 " (…) *hay que erradicar la práctica de algunos jueces de instrucción, totalmente irregular, de no aceptar atestados conteniendo peticiones de la Policía Judicial mediante el acto no jurídico, de devolución en mano del atestado, indicándoles de palabra que vayan a otro Juzgado alegando falta de competencia".*

Juez con jurisdicción penal será válida, aun cuando ulteriormente se resuelva su incompetencia territorial por el órgano superior, no vulnerando estas actuaciones el derecho al juez natural predeterminado por la Ley (STC 55/2007, de 12 de marzo y STS 277/2003, de 23 de enero). La discrepancia interpretativa sobre la normativa legal que atribuye la competencia entre órganos de la jurisdicción penal ordinaria no constituye infracción del derecho al juez natural predeterminado por la Ley, salvo que la atribución de la competencia sea arbitraria y el juez haya actuado conociendo su falta de competencia, en cuyo caso si podría darse lugar a la nulidad de lo actuado por la vulneración de ese derecho fundamental[133].

Cuando los hechos ilícitos se hayan cometido parcialmente en España o se manifiesten los efectos de la acción delictiva en nuestro país, los tribunales españoles tendrán competencia para investigar y enjuiciar aquellos delitos según la ley española.

Con base en ello se siguen en nuestro país procedimientos judiciales por actuaciones parciales de una actividad delictiva proyectada desde otros países y con efectos no solo en España, sino también en otros Estados. Tal es el caso en los fraudes bancarios a través de *phsising*, en relación con los intermediarios captados en territorio nacional y que han desarrollado su actuación ilícita en nuestro país, aun cuando esté integrada en el marco de una operación planificada y coordinada más allá de nuestra fronteras[134].

[133] VILLAGÓMEZ MUÑOZ, A. "Otras medidas de investigación limitativas de derechos (…) ob. cit. pág. 12.

[134] ATS 19 de febrero de 2014 (cuestión de competencia 20768/2013) en el ciberdelito denominado phising la competencia es del Juzgado del lugar donde se ingresa el dinero en la cuenta del "mulero" y desde donde se hace la transferencia al extranjero, al desconocerse el lugar donde se obtuvieron ilícitamente los datos de la cuenta de la víctima. Nos encontramos en presencia de cuatro ubicaciones:
a) Lugar de emisión de los correos : A efectos de la investigación, éste sería el lugar en el que se inicia la trama defraudatoria, aunque a efectos de la investigación de los hechos resulta irrelevante por las propias indicaciones que hace la policía en torno al origen de este tipo de cuentas de correo y su anonimato.
b) Lugar de actuación y de residencia de la intermediaria: donde recibe las transferencias en su cuenta corriente, de donde se extrae materialmente el dinero del circuito bancario, y desde donde se efectúan los envíos de metálico a los destinos en el extranjero con arreglo a las instrucciones recibidas. A los efectos de la investigación del este lugar cobra trascendencia, es el lugar donde la investigación policial puede tener algún efecto, al poderse operar bien sobre el equipo informático de la imputada, bien sobre las empresas de envíos de dinero metálico al extranjero; en definitiva donde la instrucción puede alcanzar, dentro de lo posible, más eficacia.
c) Lugar de residencia de las víctimas del delito y domicilio de la entidad bancaria donde tienen abiertas sus cuentas corrientes. Estos son lugares, a efectos de la instrucción de la causa, absolutamente irrelevantes. La mecánica operativa desplegada a través de internet prescinde de la localización física de la concreta sucursal bancaria en la que la víctima tenga situada su cuenta corriente. Se opera desde la red

Cuando estas conductas trasvasan los límites fronterizos estatales surgen problemas porque los mecanismos de cooperación internacional no siempre funcionan con la celeridad necesaria, dando lugar en ocasiones a la pérdida de la eficacia de la investigación[135].

Los principales problemas que suscitan estas investigaciones derivan de carencias normativas, en ocasiones de carácter sustantivo por falta de tipificación penal de algunas conductas lesivas, y en otras, de carácter procesal[136].

Cuestión distinta es la relacionada con la aplicación de la jurisdicción española en casos de delitos cometidos fuera del territorio nacional. En esos casos la competencia de los Tribunales españoles se encuentra definida en el artículo 23 de la Ley Orgánica del Poder Judicial[137]. Los delitos comprendidos en los apartados 2 y 3 del artículo 23

---

y a través de claves y procedimientos informáticos. La operativa que no precisa la presencia física del autor en las localidades donde se encuentran ubicadas dichas cuentas corrientes.
d) Lugar de emisión de la orden de transferencia . Puede ser relevante para la investigación. Normalmente no coincidirá con ninguno de los lugares anteriormente considerados, ni los domicilios de las cuentas corrientes de donde se extrae el dinero, ni el domicilio de la cuenta corriente del intermediario.

[135] FLORES PRADA, I. "Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia". Revista Electrónica de Ciencia Penal y Criminología nº 17-21, 2015. pág. 10.

[136] No obstante, se han ido produciendo importantes avances en el ámbito sustantivo con el fin de adaptar la legislación a las exigencias derivadas de estas nuevas formas de delincuencia. Ya supuso un gran avance la reforma efectuada por la Ley Orgánica 5/2010 que además de actualizar el CP, tipificando nuevos comportamientos vinculados a la utilización de las TIC y adaptar otras figuras delictivas ya existentes a las peculiaridades de su comisión a través de los medios tecnológicos, efectuó la transposición al CP de la Decisión Marco 2005/222/JAI (sustituida por la Directiva 2013/40, relativa a los ataques contra los Sistemas de Información). También la reforma efectuada por la LO 1/2015 de 30 de marzo, que modificó el Código Penal en los delitos contra la libertada sexual para incorporar la Directiva 2011/93, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituyó la Decisión Marco 2004/68/JAI del Consejo. En lo que concierne a la normativa procesal, para dar solución a muchas de las cuestiones que se planteaban en la investigación tecnológica *Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica* introdujo nuevas técnicas de investigación en la Ley de Enjuiciamiento Criminal. *Vid*. Apéndice normativo

[137] De acuerdo con dicho precepto y en relación con los ciberdelitos serán competencia de la jurisdicción española
Art 23.2. Los que hayan sido cometidos fuera del territorio nacional, siempre que los responsables fueran españoles o extranjeros que hayan adquirido la nacionalidad española con posterioridad a la comisión del hecho y concuerdan los siguientes requisitos
-que el hecho sea punible en el lugar de ejecución (salvo alguna excepción) -
que agraviado o Ministerio Fiscal interpongan querella ante los Tribunales españoles
-que el delincuente no haya sido absuelto, indultado o penado en el extranjero y en este caso que no haya cumplido la condena
Art 23.3 Hechos cometidos fuera del territorio nacional por españoles o extranjeros cuando sean susceptibles de tipificarse según la ley española como algunos de los delitos incluidos en dicho precepto, entre los que estimamo oportuno mencionar los siguientes

LOPJ, no serán perseguibles en España cuando se haya iniciado procedimiento por Tribunal Internacional o en el Estado en el que se hubieran cometido los hechos o en el Estado de nacionalidad de la persona a la que se impute la comisión, siempre que la persona imputada no se encuentre en territorio nacional o se haya iniciado el procedimiento para la extradición de la misma al país en que se hubieran cometido los hechos o de cuya nacionalidad fueran las victimas o para ponerlo a disposición de un Tribunal Internacional.

Por regla general, el ciberdelito no tiene la consideración de delito de persecución internacional, pues no se encuentra comprendido entre los que el art. 23.4 de la LOPJ incluye en la categoría del principio de universalidad.

No obstante, algunas modalidades delictivas, como pudiera ser el sabotaje informático (aquél en el que se ataca a sistemas enteros de comunicación de datos afectando a una generalidad de personas, produciendo un evidente perjuicio en servicios esenciales para la comunidad -aeropuertos, hospitales, etc.-) podrían entrar en esta

---

a) contra la paz y la independencia del Estado
d) falsificación de la firma o estampilla reales del sello del Estado, de las firmas de los Ministros y de los sellos públicos u oficiales.
f) cualquier falsificación que perjudique directamente al crédito o intereses del Estado
Art 23.4.-Hechos cometidos por españoles o extranjeros fuera del territorio nacional susceptibles de tipificarse por la legislación española como algunos de los delitos incluidos en el precepto siempre que se cumplan las condiciones establecidas en el mismo, entre los que estimo oportuno mencionar los siguientes:
e) delitos de terrorismo, cuando concurra alguno de los siguientes requisitos:
1º. procedimiento dirigido contra un español
2º. procedimiento dirigido contra un extranjero que resida en España o contra una persona que colabore con un español o un extranjero que resida o se encuentre en España para cometer un delito de terrorismo.
3º. cometido por cuenta de persona jurídica domiciliada en España.
4º. victima de nacionalidad española cuando se cometen los hechos
5º. cometido para influir o condicionar la actuación de autoridad española.
6º. cometido contra una institución u organismos de la UE con sede en España
7º. cometido contra buque o aeronave con pabellón español.
8º. cometido contra instalaciones oficiales españolas
j) Delitos de constitución, financiación o integración en grupo u organización criminal o delitos cometidos en el seno de los mismos, siempre que se trate de grupos u organizaciones que actúen con miras a la comisión en España de un delito que este castigado con pena máxima o igual a tres años de prisión.
k) Delitos contra la libertad e indemnidad sexual cometidos sobre victimas menores de edad siempre que:
1º. que el procedimiento se dirija contra un español
2º. que el procedimiento se dirija contra un extranjero que resida en España
3º. que el procedimiento se dirija contra personas jurídicas, empresas, grupos o cualquier entidad u organización con domicilio o sede social en España
4º. que la victima sea española o tenga su residencia habitual en España en el momento de comisión de los hechos.

modalidad si van asociados a fenómenos de tipo terrorista o siempre que así lo indiquen los correspondientes Tratados Internacionales.

Por otro lado, el carácter internacional de algunos de los delitos informáticos, se aprecia claramente en el de pornografía infantil (art. 189 del CP) el cual es de persecución universal en base a una doble vía:

a) Por ser uno de los delitos "relativos a la prostitución y/o corrupción de menores (art. 23.4-d LOPJ)

b) Por establecer el art. 189.1-b del CP para los de tráfico de material pornográfico infantil que es indiferente que el mismo tenga su origen en el extranjero o fuere desconocido.

Aunque sobre la base de su persecución universal la competencia para su instrucción correspondería a los Juzgados Centrales de Instrucción (art. 65.1-e LOPJ), sin embargo, en la práctica se atribuye a los Juzgados de Instrucción en aras al ya examinado principio de ubicuidad.

En cuanto a los delitos de adoctrinamiento o adiestramiento terrorista a través de internet, conforme al artículo 575 CP, apartado 2, párrafo segundo *in fine* los hechos se entenderán cometidos en España cuando se acceda a los contenidos desde el territorio español.

2. LOS CONFLICTOS DE JURISDICCIÓN ENTRE DOS O MÁS ESTADOS PARA INVESTIGAR LOS CIBERDELITOS COMETIDOS EN PARTE FUERA DE SUS RESPECTIVOS TERRITORIOS.

Otra interesante cuestión es cómo se resuelven los conflictos de jurisdicción cuando dos o más Estados pueden investigar (y procesar al mismo autor) por ciberdelitos cometidos en parte fuera de sus respectivos territorios.

Al respecto, la Instrucción 3/2011 de la Fiscalía General del Estado, sobre el nuevo régimen de intercambio de información derivado de la Decisión del Consejo de la Unión Europea de 16 de diciembre de 2008 por la que se refuerza Eurojust, se anticipó a la *Ley 16/2015, de 7 de julio, por la que se regula el estatuto del miembro nacional de España en Eurojust, los conflictos de jurisdicción, las redes judiciales de cooperación internacional y el personal dependiente del Ministerio de Justicia en el Exterior*[138], pues trataba esta cuestión de la siguiente manera:

"Los Fiscales que en el curso de su actuación detecten la existencia de investigaciones paralelas en distintos países deberán valorar en primer lugar la necesidad o conveniencia de la concentración de las investigaciones o la preferencia por la continuación en investigaciones parciales. Cuando el tratamiento fragmentario de una investigación se considere inadecuado, especialmente en relación con operaciones que globalmente consideradas presenten mayor gravedad y por tanto sea preferible su tratamiento conjunto, deberá intentarse la concentración de las investigaciones en un solo Estado, que será aquel que se encuentre en mejores condiciones para investigar o juzgar los hechos delictivos. El acuerdo sobre la acumulación de la investigación y los procedimientos en el Estado que se encuentre en mejores condiciones para conocer debe intentarse en principio directamente, mediante la oportuna comunicación con las autoridades competentes por la vía prevista en los Tratados aplicables (Convenio sobre transmisión de procedimientos del Consejo de Europa de 1972, art. 21 del Convenio de cooperación en materia penal del Consejo de

[138] BOE núm. 162, de 8 de julio de 2015.

Europa de 1959, etc.). Sólo en el caso de que no sea posible lograr un acuerdo por ese procedimiento, surgirá la concreta obligación de comunicación a Eurojust."

La citada Instrucción 3/2011 imponía a los fiscales españoles la comunicación obligatoria a Eurojust en caso de conflictos de jurisdicción entre investigaciones paralelas en distintos Estados miembros: tanto los previsibles como los ya efectivamente planteados (los casos en que se hayan producido o sea probable que se produzcan) (art. 13.7 de la Decisión). La propia Instrucción aclaraba que no debía entenderse que procediera la comunicación en cada supuesto de conflicto de jurisdicción (positivo o negativo) sino que se trata de notificar a Eurojust los supuestos problemáticos, es decir, aquellos en que, establecidos previos contactos entre autoridades competentes, no hubiera sido posible un acuerdo sobre asunción del caso por uno solo -y al menos uno de los Estados miembros[139].

Por otra parte, existía un ámbito de especial e intensa relación con la Fiscalía por cuanto el art. 14.2 de la Ley 16/2006[140] residenciaba en el Fiscal General del Estado la recepción de las Recomendaciones de Eurojust para que se iniciaran investigaciones o se reconociera la preferencia de otra jurisdicción. En los supuestos en que se pretendiera ampliar una investigación nacional a otros investigados por una autoridad judicial de otro Estado miembro (art. 16 Ley 16/2006), podía optarse por remitirla directamente a la autoridad judicial competente o al Fiscal General[141].

[139] Esta interpretación restrictiva derivaba de las propias disposiciones de la Unión y concretamente de la Decisión Marco 2009/948/JAI del Consejo de 30 de noviembre de 2009 sobre la prevención y resolución de conflictos de ejercicio de jurisdicción en los procesos penales. Esta información se transmitía a Eurojust, previa cumplimentación del formulario, a través de la Unidad de Cooperación Internacional Fiscalía General del Estado. La Oficina Española en Eurojust disponía de una cuenta de correo electrónico específica para recibir las fichas del artículo 13 (art13ES@eurojust.europa.eu). Hasta la *Ley 16/2015, de 7 de julio*, de los once formularios remitidos desde la Fiscalía General del Estado, tres casos se habían basado en el art. 13.7.a, identificación de potenciales conflictos de jurisdicción.

[140] BOE núm. 126, de 27 de mayo de 2006 derogada por la disposición derogatoria única de la Ley 16/2015, de 7 de julio.

[141] Los datos relativos a las Recomendaciones vienen siendo recogidos en la Memoria Anual del Ministerio Fiscal, en el apartado dedicado a Cooperación Internacional. En el año 2015, se recibieron tres recomendaciones relativas a conflictos de jurisdicción 2 con Francia y 1 con Finlandia. En el año 2014, se recibió una única Recomendación; en el año 2013, se recibieron tres Recomendaciones; los años 2009 a 2012 se recibieron ocho Recomendaciones, a razón de una por año con la excepción del año 2011, en que se recibieron cinco. En todas las ocasiones salvo en una (en la que por circunstancias sobrevenidas no cabía ya hablar de mejor posición procesal por haber llegado a su fin el procedimiento en la jurisdicción

La remisión o recepción del procedimiento se lleva a cabo aplicando el único Convenio en vigor que regula de forma completa esta cuestión: el Convenio del Consejo de Europa sobre transmisión de procedimientos en materia penal de 17 de Marzo de 1972 (ratificado por España el 24 de junio de 1988), que sin embargo, establece un procedimiento de comunicación lento y obsoleto en relación con la Unión Europea.

Cuando se trata de Estados que no han ratificado el citado Convenio se acude a la regulación de "la denuncia a efectos procesales" que se recoge en el art. 21 del Convenio de 1959. Esta disposición ha sido modificada por lo dispuesto en el artículo 6.1 párrafo segundo del Convenio de 2000 que establece que: "Toda denuncia cursada por un Estado miembro cuyo objeto sea incoar un proceso ante los tribunales de otro Estado miembro con arreglo a lo dispuesto en el artículo 21 del Convenio europeo de asistencia judicial y en el artículo 42 del Tratado Benelux podrá transmitirse mediante comunicación directa entre las autoridades judiciales competentes"[142].

Mediante la Ley 16/2015, de 7 de julio, por la que se regula el estatuto del miembro nacional de España en Eurojust, los conflictos de jurisdicción, las redes judiciales de cooperación internacional y el personal dependiente del Ministerio de Justicia en el Exterior[143], por primera vez en Derecho positivo español se recogen

---

extranjera) se aceptaron por el Fiscal General las tesis planteada por Eurojust y se dio la correspondiente orden al Fiscal del caso para que plantease las mismas ante el Juzgado competente.

[142] Esta disposición se utiliza cada vez con mayor frecuencia y ha permitido resolver casos realmente relevantes. También se han transmitido procedimientos a Estados signatarios del Convenio de 1952 a través del mecanismo de la denuncia previsto en el art. 21 del Convenio de 1959.
Existe, al menos, un caso de traslado de procedimiento por ciberdelito, relativo a un asunto bilateral con Bulgaria, donde en el marco de Eurojust se creó un equipo conjunto de investigación por un Juzgado Central de Instrucción y la Fiscalía de la Audiencia Nacional que culminó con el acuerdo de transferencia a Bulgaria.

[143] http://www.eurojust.europa.eu/doclibrary/Eurojustframework/ejdecision/New%20Eurojust%20Decision%20(Council%20Decision%202009-426-JHA)/Eurojust-Council-Decision-2009-426-JHA-ES.pdf.
Se incorpora al derecho español la Decisión Marco 2009/948/JAI del Consejo, de 30 de noviembre de 2009, sobre la prevención y resolución de conflictos de ejercicio de jurisdicción en los procesos penales, y se adapta el ordenamiento jurídico a la Decisión 2009/426/JAI, de 16 de diciembre de 2008, por la que se refuerza Eurojust y se modifica la Decisión 2002/187/JAI, por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia y la Decisión 2008/976/JAI del Consejo, de 16 de diciembre de 2008, sobre la Red Judicial Europea.
Esta Decisión otorgó a los Estados miembros un plazo de dos años desde la fecha de su publicación para adaptar sus respectivos ordenamientos a sus disposiciones, de manera que desde el 4 de junio de 2011 España debería estar en condiciones de dar cumplimento a las obligaciones que de ella se derivan, sin embargo no se implementó hasta La Ley 16/2015, de 7 de julio. Hasta entonces se mantuvo por tanto plenamente vigente la Ley 16/2006, de 26 de mayo, *por la que se regulaba el Estatuto del Miembro Nacional de Eurojust y las relaciones con este órgano de la Unión Europea,* que atribuía explícitamente una serie de funciones y obligaciones al Ministerio Público español, especialmente en el ámbito de la

parámetros específicos para la determinación de los criterios a tener en consideración a la hora de establecer la jurisdicción más adecuada en interés de la Justicia. Así, el capítulo V, se dedica a los conflictos de jurisdicción en tres artículos, en los que se establece el procedimiento a seguir en tres fases:

1) Solicitud de contacto a la autoridad competente de otro Estado miembro ante la sospecha de un conflicto de jurisdicción (artículo 30). Se realizará por Auto motivado previa audiencia del Fiscal si es la Autoridad judicial o Decreto si es el Ministerio Fiscal el que cursa dicha solicitud, en el plazo de quince días desde que conste en el procedimiento español que en otro Estado miembro se está tramitando un proceso penal, ya sea en fase de instrucción o de enjuiciamiento, contra la misma persona y respecto de los mismos hechos[144]. El contacto con la autoridad competente del otro Estado miembro será directo, sin perjuicio de la posibilidad de recabar la asistencia de los puntos de contacto de la Red Judicial Europea o del miembro nacional de España en Eurojust si resultare necesario.

---

transmisión y el intercambio de información, a cuyo eficaz cumplimiento ya trataba de responder en parte la Instrucción 1/2011 de la Fiscalía General de Estado, que abordaba algunas cuestiones de carácter orgánico en relación con la cooperación penal internacional.

[144] Art. 30.5. de la Ley 16/2015, de 7 de julio.
"*La autoridad competente deberá incluir en la solicitud de contacto la siguiente información:*
a) Una descripción detallada de los hechos y circunstancias que sean objeto del proceso penal en España, o de las diligencias de investigación.
b) Tipificación de la conducta en España.
c) Datos sobre la identidad del imputado o acusado y de la detención, prisión o de las medidas cautelares que hayan sido adoptadas.
d) Datos, si procede, de las víctimas de la infracción penal y medidas de protección que hayan sido adoptadas en relación con las mismas.
e) Fase alcanzada en el proceso penal español, con testimonio de las resoluciones judiciales que concreten la imputación realizada y los motivos racionales de criminalidad apreciados por el juez instructor, así como, en su caso, testimonio del escrito de acusación presentado por el Ministerio Fiscal y por las demás partes acusadoras personadas.
f) Datos de contacto de la autoridad judicial responsable en España de la instrucción, del enjuiciamiento o del fiscal responsable de las diligencias de investigación así como, si procediere, del punto de contacto de la Red Judicial Europea o del miembro nacional de España en Eurojust que pueda auxiliar a las autoridades judiciales en el intercambio de información en relación con este eventual conflicto de jurisdicción.
g) Asimismo la autoridad competente española podrá facilitar información adicional relativa a las pruebas o diligencias de investigación que consten practicadas en el procedimiento español o a las dificultades que se hayan planteado o sea probable que surjan en la investigación o enjuiciamiento de la causa en España.
En caso de no poder facilitar la información detallada en este apartado por entender que de hacerlo se perjudicarían los intereses fundamentales de seguridad nacional o se pondría en peligro la seguridad de las personas, en los términos previstos en el artículo 25, se hará constar expresamente en la consulta la concurrencia de estas excepciones. El secreto de las actuaciones no afectará a esta obligación de consulta, en los términos previstos en el artículo 24.3 de esta Ley."

2) Respuesta a la solicitud de contacto ante un eventual conflicto de jurisdicción (artículo 31). Se realizará por cualquier medio que deje constancia escrita en el plazo razonable indicado por dicha autoridad o, en su defecto, en el plazo de quince días desde la recepción de la solicitud. La autoridad competente tendrá la obligación de responder, en todo caso, a la solicitud de información cursada y su respuesta contendrá, cuando proceda, la información detallada en el apartado 5 del artículo anterior, salvo que perjudique los intereses fundamentales de seguridad nacional o ponga en peligro la seguridad de las personas en los términos previstos en el artículo 25, en cuyo caso se hará constar expresamente la concurrencia de estas excepciones en la respuesta que se facilite. El secreto de las actuaciones no afectará a la obligación de contestar, en los términos del artículo 24.3 de esta Ley.

3) Decisión en relación con el conflicto de jurisdicción (artículo 32). Una vez entablado contacto directo con la autoridad competente de otro Estado miembro y confirmada la tramitación paralela de dos procesos penales contra la misma persona y respecto de los mismos hechos, el órgano judicial oirá al Ministerio Fiscal y demás partes personadas, por plazo común de diez días, sobre si procede la sustanciación de ambos procedimientos penales en un mismo Estado miembro y sobre los criterios que concurren para que la autoridad judicial española ceda o no la jurisdicción a otro Estado miembro.

Se promoverá el consenso con la autoridad competente del otro Estado miembro pero en caso de que no lleguen a un acuerdo se podrá solicitar un dictamen escrito no vinculante del colegio de Eurojust, que a pesar de que no tiene fuerza vinculante para resolver el conflicto de jurisdicción entre Estados, su importancia no debe ser minimizada. Tras ello, el juez o tribunal resolverá, por auto motivado dictado en el plazo de cinco días, sobre la continuación o no del procedimiento ante la jurisdicción española.

Por último, para la resolución del conflicto de jurisdicción se tendrán en cuenta los siguientes criterios:

a) Residencia habitual y nacionalidad del imputado.

b) Lugar en el que se ha cometido la mayor parte de la infracción penal o su parte más sustancial.

c) Jurisdicción conforme a cuyas reglas se han obtenido las pruebas o lugar donde es más probable que éstas se obtengan.

d) Interés de la víctima.

e) Lugar donde se encuentren los productos o efectos del delito y jurisdicción a instancia de la cual han sido asegurados para el proceso penal.

f) Fase en la que se encuentran los procesos penales sustanciados en cada Estado miembro.

g) Tipificación de la conducta delictiva y pena con la que esta viene castigada en la legislación penal de los distintos Estados miembros implicados en el conflicto de jurisdicción.

CAPÍTULO CUARTO

INSTRUMENTOS DE COOPERACIÓN INTERNACIONAL EN MATERIA DE CIBERDELINCUENCIA.

Dado que en muchas ocasiones el ciberdelito es un delito transfronterizo, la obtención de "pruebas" de la comisión de los mismos no sólo se obtienen en territorio español, sino que en muchos casos es necesario acudir a instancias internacionales para investigar los rastros dejados en el entorno electrónico, telemático o virtual o bien para solicitar alguna diligencia necesaria para el aseguramiento de las pruebas.

El Convenio sobre Ciberdelincuencia establece en el artículo 23 los principios generales relativos a la cooperación internacional[145]

Entre de los instrumentos de cooperación internacional en materia de ciberdelincuencia, distinguimos:

1. ASISTENCIA JUDICIAL.[146]

El Convenio de Ciberdelincuencia dedica el Título 3 a los principios generales relativos a la asistencia mutua, señalando en su artículo 25.1 y 2[147]:

[145] Dispone: "*Las Partes cooperarán con arreglo a lo dispuesto en el presente capítulo, aplicando para ello los instrumentos internacionales relativos a la cooperación internacional en materia penal, acuerdos basados en la legislación uniforme o recíproca y en su propio derecho nacional, de la forma más amplia posible, con la finalidad de investigar los procedimientos concernientes a infracciones penales vinculadas a sistemas y datos informáticos o para recoger pruebas electrónicas de una infracción penal".*

[146] Dentro de la Unión Europea, hay que destacar la importancia de EUROJUST, como órgano de la Unión Europea encargado del refuerzo de la cooperación judicial entre los Estados miembros, mediante la adopción de medidas estructurales que facilitan la mejor coordinación de las investigaciones y las actuaciones judiciales que cubren el territorio de más de un Estado miembro.

"1. Las Partes acordarán llevar a cabo una asistencia mutua lo más amplia posible al objeto de investigar los procedimientos concernientes a infracciones penales vinculadas a sistemas y datos informáticos o al de recoger pruebas electrónicas de una infracción penal.

2. Las Partes adoptarán las medidas legislativas o de otro tipo que estimen necesarias para dar cumplimiento a las obligaciones establecidas en los artículos 27 a 35".

Establece además la posibilidad de dar informaciones espontáneas (art. 26 CSC) obtenidas en el marco de las investigaciones que puedan ayudar a la parte destinataria a iniciar o a concluir satisfactoriamente las investigaciones o procedimientos relativos a las infracciones dispuestas en el Convenio y un procedimiento aplicable para el caso de que no exista tratado internacional aplicable entre las partes que requieren de asistencia judicial (art. 27 CSC), respetando la confidencialidad y la restricción de uso de los datos cedidos (art. 28 CSC).

De gran importancia para la investigación de los ciberdelitos son las medidas establecidas en la Sección 2 del Capítulo III del Convenio de ciberdelincuencia sobre la asistencia en materia de medidas cautelares, tales como la conservación inmediata de datos informáticos almacenados (art. 29 CSC), la comunicación inmediata de los datos informáticos conservados (art. 30 CSC), sobre la asistencia en relación a los poderes de investigación concerniente al acceso a datos informáticos almacenados (art. 31 CSC), al acceso transfronterizo a los datos informáticos almacenados, con consentimiento o de libre acceso (art. 32 CSC), a la asistencia para la recogida en tiempo real de datos de

147 Convenio de Ciberdelincuencia, artículo 25.3. Las Partes podrán, en caso de emergencia, formular una demanda de colaboración, a través de un medio de comunicación rápido, como el fax o el correo electrónico, procurando que esos medios ofrezcan las condiciones suficientes de seguridad y de autenticidad (encriptándose si fuera necesario) y con confirmación posterior de la misma si el Estado requerido lo exigiera. Si el Estado requerido lo acepta podrá responder por cualquiera de los medios rápidos de comunicación indicados.

Salvo disposición en contrario expresamente prevista en el presente capítulo, la colaboración estará sometida a las condiciones fijadas en el derecho interno del Estado requerido o en los tratados de colaboración aplicables y comprenderá los motivos por los que el Estado requerido puede negarse a colaborar. El Estado requerido no podrá ejercer su derecho a rehusar la colaboración en relación a las infracciones previstas en los artículos 2 a 11, alegando que la demanda se solicita respecto a una infracción que, según su criterio, tiene la consideración de fiscal.

Conforme a lo dispuesto en el presente capítulo, el Estado requerido estará autorizado a supeditar la colaboración a la exigencia de doble incriminación. Esa condición se entenderá cumplida si el comportamiento constitutivo de la infracción - en relación a la que se solicita la colaboración - se encuentra previsto en su derecho interno como infracción penal, resultando indiferente que éste no la encuadre en la misma categoría o que no la designe con la misma terminología.

tráfico (art. 33 CSC) y por último a la asistencia en materia de interceptación de datos relativos al contenido (art. 34 CSC).

En el ordenamiento español no existe una ley de cooperación judicial en materia de ciberdelincuencia. Tan solo el artículo 276 de la Ley Orgánica del Poder Judicial que hace referencia a que las peticiones de cooperación internacional se tramitarán de conformidad con lo previsto en los tratados internacionales, las normas de la Unión Europea y las leyes españolas que resulten de aplicación. De tal modo que la base aplicable está constituida por los convenios internacionales de los que España es parte[148]que en el ámbito europeo, son:

- Convenio Europeo de Asistencia Judicial en Materia Penal, hecho en Estrasburgo el 20 de abril de 1959[149].
- Convenio de aplicación del Acuerdo de Schengen de 19 junio de 1990[150] .
- Convenio Europeo relativo a la Asistencia Judicial en Materia Penal entre los Estados miembros de la Unión, hecho en Bruselas el 29 de mayo de 2000[151].

Fuera del ámbito europeo habrá que acudir a los convenios existentes o, en su defecto, a la reciprocidad (277 LOPJ).

Las autoridades competentes y la forma para recibir o reenviar las solicitudes varían en función del instrumento internacional que se aplique:

[148] La Fiscalía General del Estado, el Consejo General del Poder Judicial y el Ministerio de Justicia han elaborado un instrumento muy útil para todos los operadores jurídicos en materia de cooperación judicial internacional. Se trata de una herramienta informática (www.prontuario.org) que proporciona información sobre todos los tratados firmados por España y los instrumentos europeos en materia de cooperación judicial internacional además de información práctica sobre puntos de contacto de la Red Judicial Europea y Eurojust. La información se complementa con formularios elaborados por estas instituciones y con los modelos estándar de los instrumentos de reconocimiento mutuo.

[149] Ratificado por España el 14 de julio de 1982, BOE núm. 223, de 17 de septiembre de 1982.

[150] Ratificado por España el 23 de julio de 1993, BOE núm. 81, de 5 de abril de 1994.

[151] Ratificado por España el 27 de enero de 2003, entró en vigor el 23 de agosto de 2005. BOE núm. 258, de 28 de octubre de 2005.

Así, caso de que se aplique el Convenio Europeo relativo a la Asistencia Judicial en Materia Penal entre los Estados miembros de la Unión del año 2000, las solicitudes han de remitirse directamente entre las autoridades judiciales competentes sin necesidad de tramitarlas a través de los Ministerios correspondientes[152] (se abandona así la comisión rogatoria y se autoriza la remisión directa). Se destaca que permite la realización de videoconferencias entre los países que lo han ratificado y también la asistencia entre dichos países con la finalidad de practicar intervenciones telefónicas. Cuando España es el país requerido para la práctica de la intervención telefónica la competencia corresponde al Juzgado Central de Instrucción. De otra parte, este Convenio determina que el acto de auxilio judicial se practicará de acuerdo con las formalidades propias del Estado requerido, pero también permite que el Estado requirente solicite que se cumplimente alguna formalidad específica de su legislación cuando resulte imprescindible para que el acto surta efectos jurídicos en el mismo[153]. El problema más importante radica en que este Convenio no ha sido ratificado por todos los países miembros.

En el Convenio de aplicación del Acuerdo de Schengen de 19 junio de 1990[154], se establecen una serie de formularios para la práctica de diversas diligencias, que se practicarán conforme a lo dispuesto por el estado requirente, que determinará en qué condiciones han de practicarse (*vid*. arts 48 a 53 del Convenio de aplicación del Acuerdo de Schengen).

En el caso de que las solicitudes de asistencia judicial se tramiten sobre la base del Convenio Europeo de Asistencia Judicial en Materia Penal de 1959 o en el marco de los distintos Convenios bilaterales firmados por España sobre la materia, salvo que exista Convenio aplicable que permita la comunicación directa entre autoridades judiciales, tanto la remisión como recepción de las solicitudes se realiza a través de

[152] El art. 6 del Convenio de Asistencia Judicial en Materia Penal de 29-5-2000 permite la comunicación directa entre autoridades judiciales "*Las solicitudes de asistencia judicial ... se efectuarán ... directamente entre las autoridades judiciales que tengan competencia jurisdiccional para formularlas y ejecutarlas, y se responderán del mismo modo, salvo que en el presente artículo se disponga lo contrario*".

[153] Se detectan algunos problemas prácticos en la ejecución del Convenio de Asistencia Judicial en Materia Penal de 29-5-2000, porque no regula cual de los dos países (requirente o requerido) debe proveer el intérprete y el abogado.

[154] Completa al Convenio Europeo de Asistencia Judicial en Materia Penal de 20 de abril de 1959.

comisión rogatoria de las Autoridades Centrales (en el caso de España del Ministerio de Justicia y, en concreto, a través de la Subdirección General de Cooperación Jurídica Internacional). Y deberá establecerse en la comisión rogatoria la forma en la que se ha de practicar la diligencia para que tenga validez en nuestro derecho interno.

En los casos en los que para la tramitación de las solicitudes de asistencia judicial se aplica el principio de reciprocidad, su envío y recepción se realiza a través de la vía diplomática[155].

No obstante, habrá que tener en cuenta la Directiva 2014/41/UE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a la Orden Europea de Investigación en materia penal, que aún no se ha transpuesto a nuestro derecho interno, porque sustituye, a partir del 22 de mayo de 2017, a las disposiciones correspondientes de convenios ya citados aplicables a las relaciones entre los Estados miembros vinculados por la presente Directiva. La orden europea de investigación (OEI) será de gran importancia para la investigación del ciberdelito es pues establece un régimen único para la obtención de pruebas en los casos de dimensión transfronteriza[156].

Por lo que se refiere a los cauces de comunicación en la tramitación de las solicitudes de asistencia judicial, el medio más utilizado es el correo ordinario o por mensajería, utilizándose también el fax y el correo electrónico. Las autoridades judiciales competentes para recibir (o reenviar) solicitudes de asistencia judicial en general en la investigación de todo tipo de delitos (y, por tanto también en investigaciones de ciberdelitos) son los jueces de instrucción y los fiscales[157].

---

[155] El uso de la vía diplomática (embajadas y consulados) puede resultar conveniente en casos tales como la cumplimentación de las comparecencias "apud acta", pero que resulta cuestionable su utilización para la práctica de diligencias instructoras de relevancia o calado, ya que existe riesgo de nulidad de las actuaciones al obviarse la aplicación de los instrumentos establecidos en la normativa internacional vigente.

[156] *Vid*. apéndice de normativa. La OEI se ejecutará en cada Estado miembro sobre la base del principio de reconocimiento mutuo y se regirá por el derecho del estado de ejecución.

[157] En concreto en relación al Ministerio Fiscal, tiene atribuida la promoción y la prestación del auxilio judicial internacional previsto en leyes tratados y convenios (art. 3.15 del Estatuto Orgánico del Ministerio Fiscal) y por declaración efectuada al Convenio de Asistencia Mutua en Materia Penal de 1959 (extensiva al Convenio 2000), tiene la consideración de autoridad judicial a los efectos de cooperación internacional.
La Fiscalía General del Estado, en el ejercicio de su potestad auto organizativa así como para garantizar el principio de unidad de actuación consagrado por la Constitución ha dictado numerosas instrucciones, que

No hay procedimientos o condiciones específicas en relación con las diversas clases solicitudes de asistencia judicial relacionadas con la ciberdelincuencia[158]. Las solicitudes urgentes se remiten a su destinatario en cuanto se reciben en este Departamento. Asimismo, se adelantan a los órganos competentes para su ejecución por correo electrónico o fax, remitiendo el original a la mayor brevedad posible tal y como establecen los diferentes instrumentos aplicables. El periodo medio de ejecución de las citadas solicitudes es de 4 meses. Los motivos más corrientes de las solicitudes de asistencia judicial son para la identificación de cuentas IP, remisión de información sobre cuentas de correo electrónico y datos sobre conexiones[159].

---

son de obligado cumplimiento para todos los fiscales, con el propósito de ajustar la actuación de los miembros de la Carrera Fiscal a las disposiciones reguladoras de Eurojust. En concreto debe citarse:
- La *Instrucción 3/2001, de 28 de junio, sobre los actuales mecanismos y modalidades de asistencia judicial internacional en materia penal*, que recopila para los fiscales españoles la normativa europea y los mecanismos existentes en materia de cooperación judicial internacional penal, con mención expresa de la Red Judicial Europea y Eurojust;
- L*a Instrucción 2/2003, de 11 de julio, sobre actuación y organización de las Fiscalías en materia de Cooperación Judicial Internacional,* que crea el Servicio Especial de Cooperación Judicial Internacional y el sistema informático para el registro de asuntos de cooperación internacional; delimita las funciones de los fiscales integrantes de la Red de Fiscales de Cooperación Judicial Internacional; resuelve problemas comunes inherentes a la ejecución de comisiones rogatorias y estableces criterios de coordinación para la ejecución de solicitudes de auxilio en territorio de varias fiscalías.
- La *Instrucción 2/2007 sobre la organización de la Sección de Cooperación Internacional de la Secretaría Técnica de la Fiscalía General del Estado y el ejercicio de las funciones que atribuye al Ministerio Público la ley 16/2006, de 26 de mayo por la que se regula el Estatuto del Miembro Nacional de Eurojust y las relaciones con este órgano de la Unión Europea*;
- La *Instrucción 1/2011 sobre las funciones y facultades del Fiscal de Sala de Cooperación Penal Internacional*, que atribuye al Fiscal de Sala de Cooperación Penal Internacional (en cuanto Jefe de la Unidad de Cooperación Internacional de la Fiscalía General del Estado) las funciones relativas al auxilio judicial internacional, incluyendo las actuaciones derivadas de las actividades de Eurojust, de las relaciones con la OLAF, con la Red Judicial Europea o con Iber-Red y, en consecuencia, la dirección y coordinación de las actividades de la Red de Fiscales de Cooperación Internacional. Esta Instrucción, asimismo señala que el Fiscal de Sala "podrá contribuir a cubrir las exigencias organizativas demandadas del Ministerio Fiscal para dar cumplimiento a las previsiones de la Decisión 2009/426/JAI;
- La *Instrucción 3/2011, sobre el nuevo régimen de intercambio de información derivado de la Decisión del consejo de la Unión Europea de diciembre de 2008, por la que se refuerza Eurojust*.

[158] Es útil utilizar la REJUE (Red Judicial Europea) para intercambiar información sobre el seguimiento de las comisiones rogatorias remitidas a otros países europeos e IBERRED (Red Iberoamericana de Cooperación Jurídica Internacional) para agilizar la tramitación y cumplimentación de las comisiones rogatorias que se solicitan a países iberoamericanos.

[159] VILLODRE LÓPEZ, J. "Cooperación Judicial Penal" Ponencia presentada el día 20 de abril de 2016 en las IV Jornadas de Derecho Procesal organizadas por la 7ª Zona de la Guardia Civil de Catalunya, sobre Cooperación Judicial Penal.

2. RECONOCIMIENTO MUTUO.

El principio de reconocimiento mutuo, basado en la confianza entre los Estados miembros y consagrado en el Consejo Europeo de Tampere como la "piedra angular" de la cooperación judicial civil y penal en la Unión Europea, ha supuesto una auténtica revolución en las relaciones de cooperación entre los Estados miembros, al permitir que aquella resolución emitida por una autoridad judicial de un Estado miembro sea reconocida y ejecutada en otro Estado miembro, salvo cuando concurra alguno de los motivos que permita denegar su reconocimiento.

El marco normativo actual está integrado por la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea (y la Ley Orgánica 6/2014, de 29 de octubre, complementaria de la anterior, por la que se modifica la LOPJ)[160].

[160] Esta ley incorpora a nuestro ordenamiento jurídico:
- La Decisión Marco 2008/909/JAI, de 27 de noviembre de 2008, relativa a la aplicación del principio de reconocimiento mutuo de sentencias en materia penal por las que se imponen penas u otras medidas privativas de libertad a efectos de su ejecución en la Unión Europea;
- la Decisión Marco2008/947/JAI, de 27 de noviembre de 2008, relativa a la aplicación del principio de reconocimiento mutuo de sentencias y resoluciones de libertad vigilada con miras a la vigilancia de las medidas de libertad vigilada y las penas sustitutivas;
- la Decisión Marco 2008/978/JAI, de 18 de diciembre de 2008, relativa al exhorto europeo de obtención de pruebas para recabar objetos, documentos y datos destinados a procedimientos en materia penal;
- la Decisión Marco 2009/299/JAI, de 26 de febrero de 2009, por la que se modifican las Decisiones Marco 2002/584/JAI, 2005/214/JAI, 2006/783/JAI, 2008/909/JAI y 2008/947/JAI, destinada a reforzar los derechos procesales de las personas y a propiciar la aplicación del principio de reconocimiento mutuo de las resoluciones dictadas a raíz de juicios celebrados sin comparecencia del imputado;
- la Decisión Marco 2009/829/JAI, de 23 de octubre de 2009, relativa a la aplicación, entre Estados miembros de la Unión Europea, del principio de reconocimiento mutuo a las resoluciones sobre medidas de vigilancia como sustitución de la prisión provisional;
- la Directiva 2011/99/UE, de 13 de diciembre de 2011, sobre la orden europea de protección.
Y además da una nueva redacción a los instrumentos que ya se habían anteriormente transpuesto, así:
- La Decisión Marco 2002/584/JAI, relativa a la orden europea y a los procedimientos de entrega entre Estados miembros, incorporada inicialmente al Derecho español a través de la Ley 3/2003, de 14 de marzo, sobre la orden europea de detención y entrega y la Ley Orgánica 2/2003, de 14 de marzo, complementaria de la anterior.
- La Decisión Marco 2003/577/JAI, de 22 de julio de 2003, relativa a la ejecución en la Unión Europea de las resoluciones de embargo preventivo de bienes y aseguramiento de pruebas, incorporada inicialmente al Derecho español a través de la Ley 18/2006, de 5 de junio, para la eficacia en la Unión Europea de las resoluciones de embargo y aseguramiento de pruebas en procedimientos penales y la Ley Orgánica 5/2006, de 5 de junio, complementaria de la anterior, por la que se modifica la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.
- La Decisión Marco 2005/214/JAI, de 24 de febrero de 2005, relativa a la aplicación del principio de reconocimiento mutuo de sanciones pecuniarias, transpuesta anteriormente en España mediante la Ley 1/2008, de 4 de diciembre, para la ejecución en la Unión Europea de resoluciones que impongan sanciones pecuniarias y la Ley Orgánica 2/2008, de 4 de diciembre,

La ley se divide en diez Títulos entre los que se destaca la Orden Europea de detención y entrega, la de protección y el Título X que era el dedicado al exhorto europeo de obtención de pruebas[161] que ha sido derogado expresamente[162] al ser sustituido por la Directiva 2014/41/UE del Parlamento Europeo y del Consejo relativa a la Orden Europea de Investigación (OEI). No obstante, esta última directiva no ha sido transpuesta aún a nuestro derecho interno, por lo que en esta materia nos encontramos con un vacío legal hasta que no se produzca su transposición teniendo como fecha límite el 22 de mayo de 2017.

Conviene en este aspecto poner de manifiesto que, salvo en el caso de la Orden Europea de Detención y Entrega (OEDE), los demás instrumentos de reconocimiento mutuo (con particular referencia a los que ya están implementados en nuestra legislación desde hace años y, singularmente, en lo relativo al embargo y aseguramiento de pruebas y al decomiso) han tenido una aplicación muy limitada en lo relativo al auxilio judicial activo por parte de las autoridades judiciales españolas.

---

de modificación de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, complementaria de la anterior.

- La Decisión Marco 2006/783/JAI, de 6 de octubre de 2006, relativa a la aplicación del principio de reconocimiento mutuo de resoluciones de decomiso, transpuesta anteriormente en nuestro país, a través de la Ley 4/2010, de 10 de marzo, para la ejecución en la Unión Europea de resoluciones judiciales de decomiso y la Ley Orgánica 3/2010, de 10 de marzo, de modificación de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y complementaria de la anterior.

[161] AGUILERA MORALES, M. "El exhorto europeo de investigación: a la búsqueda de la eficacia y la protección de los derechos fundamentales en las investigaciones penales transfronterizas". Boletín del Ministerio de Justicia nº 2145, Agosto de 2012 www.mjusticia.es/bmj
Artículo 186 de la Ley lo define como una resolución judicial emitida por la autoridad competente de un Estado miembro con objeto de recabar objetos, documentos y datos de otro Estado miembro para su uso en un proceso penal.

[162] El Reglamento (UE) 2016/95 del Parlamento Europeo y del Consejo de 20 de enero de 2016 por el que se derogan determinados actos en el ámbito de la cooperación policial y judicial en materia penal, al considerar que la Decisión Marco 2008/978/JAI del Consejo relativa al exhorto europeo de obtención de pruebas fue sustituida por la Directiva 2014/41/UE del Parlamento Europeo y del Consejo relativa a la orden europea de investigación.

3. ENTREGA Y EXTRADICIÓN.

Procede la Orden Europea de Detención y entrega, según la Decisión Marco 2002/584/JAI, relativa a la orden europea y a los procedimientos de entrega entre Estados miembros y la Ley 23/2014 de 20 de noviembre de reconocimiento mutuo de resoluciones penales en la Unión Europea, en los casos siguientes:

a) Con el fin de proceder al ejercicio de acciones penales, por aquellos hechos para los que la ley penal española señale una pena o una medida de seguridad privativa de libertad cuya duración máxima sea, al menos, de doce meses, o de una medida de internamiento en régimen cerrado de un menor por el mismo plazo.

b) Con el fin de proceder al cumplimiento de una condena a una pena o una medida de seguridad no inferior a cuatro meses de privación de libertad, o de una medida de internamiento en régimen cerrado de un menor por el mismo plazo.

Respecto a la extradición, el Convenio de ciberdelincuencia establece los principios generales relativos a la extradición en materia de ciberdelincuencia (art. 24), entre los que se incluye que la extradición quedará sometida a las condiciones establecidas en el derecho interno. En España está regulada en la Ley 4/1985, de 21 de marzo, de extradición pasiva, que establece en su artículo 2 que *"se podrá conceder la extradición por aquellos hechos para los que las Leyes españolas y las de la parte requirente señalen una pena o medida de seguridad cuya duración no sea inferior a un año de privación de libertad en su grado máximo o a una pena más grave; o cuando la reclamación tuviere por objeto el cumplimiento de condena a una pena o medida de seguridad no inferior a cuatro meses de privación de libertad por hechos también tipificados en la legislación española".*

Los numerosos tratados de extradición suscritos por España contienen normativa específica al respecto de los delitos que dan lugar a la extradición.

Son competentes para la recepción de las OEDE los Juzgados Centrales de Instrucción y el Ministerio de Justicia lo es para las extradiciones. Por lo que se refiere a

la emisión de las OEDE y extradiciones son competentes los Juzgados y Tribunales españoles competentes por razón del delito cometido.

No hay ninguna especialidad en la tramitación OEDE o extradiciones por tipo de delito.

En el ámbito de la OEDE es posible acordar la prisión provisional mientras se sustancia el procedimiento de entrega con la finalidad de garantizar el buen fin del expediente de entrega[163]. La prisión preventiva ha de someterse a las mismas reglas y condiciones que en un supuesto de investigación nacional. En el ámbito de los procedimientos de extradición conforme a la Ley de extradición pasiva es también posible acordar la prisión provisional si el Estado reclamante así lo solicita; esta prisión provisional deberá dejarse sin efecto si a los 40 días de haberse acordado el Estado reclamante no ha presentado en forma la reclamación extradicional[164].

[163] Al formalizar la Orden Europea de Detención y Entrega no resulta conveniente dictar Auto de Detención, por los problemas prácticos que genera, siendo preferible dictar Auto de Prisión del art. 539 LECrim estableciendo la celebración de la comparecencia prevista en el art. 505 LECrim en las 48 horas siguientes a su detención.

[164] Los tratados bilaterales suscritos por España contienen también normativa específica en relación a la prisión provisional, siendo que el plazo de presentación de la documentación extradicional señalado puede variar según el tratado en cuestión, de aplicación preferente, evidentemente, a la Ley de extradición pasiva. Se han constatado situaciones en que la documentación extradicional no ha llegado dentro del plazo fijado y, en consecuencia, la persona reclamada ha tenido que ser puesta en libertad a la espera de la sustanciación del procedimiento.

SEGUNDA PARTE

LA INVESTIGACIÓN Y PRUEBA EN LOS CIBERDELITOS

CAPÍTULO QUINTO

SUJETOS Y ÓRGANOS DE LA INVESTIGACIÓN DE LOS CIBERDELITOS.

Sin duda, la mayor dificultad que surge *prima facie* en la investigación penal de los ciberdelitos es que son necesarios conocimientos técnicos especializados, procedimientos adecuados e instrumentos legales suficientes[165]. Por ello, el primer rasgo que destaca al afrontar los problemas que plantea la ciberdelincuencia es la necesidad de poseer un conocimiento especializado para llevar a buen término su investigación.

Las Recomendaciones del Consejo de Europa de 1989 y 1995 (R (89) 9 y R (95) 13) ya subrayaron la necesidad de que las autoridades nacionales, policiales o gubernativas, encargadas de aplicar la ley establecieran departamentos u oficinas especializadas en delitos informáticos, dotadas de personal adecuado y de equipos programas informáticos apropiados, personal capacitado y con conocimientos técnicos al día, y programas de especialización. Muchos Estados, entre ellos España, crearon departamentos policiales especializados en delincuencia informática[166], fiscales especializados en ciberdelitos, e incluso en algunos países se han preparado diversos manuales con instrucciones técnicas, forenses y de procedimiento sobre la manera de llevar a cabo una investigación para reducir la pérdida de pruebas y garantizar la admisibilidad de éstas ante los tribunales[167].

---

[165] ROVIRA DEL CANTO, E. *Las nuevas pruebas telemática y digitales* (…) ob. cit. pág. 277-326.

[166] Así la Unidad de Delincuencia Telemática de la Guardia Civil operativa desde 1996, o la Unidad de Investigación Tecnológica del Cuerpo Nacional de Policía, formalmente constituida en 1995, y las incipientes unidades especializadas en Cuerpos Policiales Autonómicos como en la Ertzaina o en los Mossos d'Esquadra.

[167] Como en EE.UU. con su conocido manual "*Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations"* de 2009. https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf

1. FISCALES DE CRIMINALIDAD INFORMÁTICA.

Sin perjuicio del actual modelo de instrucción judicial, el Ministerio Fiscal desarrolla en nuestro país una importante labor de colaboración con el órgano judicial en la fase de investigación del delito (artículo 773 de la LECrim), máxime si se tiene en cuenta que no existen en España órganos judiciales especializados para la investigación de los ciberdelitos. Por contra, en la Fiscalía se han dado pasos muy importantes en este sentido como la Instrucción 2/2011 de la Fiscalía General del Estado, *"Sobre el Fiscal de Sala de Criminalidad Informática y las Secciones de criminalidad informática de las fiscalías"* por la que se crean estas figuras.

Se trata de un servicio de carácter nacional dirigido y coordinado por un Fiscal de Sala con competencia en todo el territorio del Estado[168]y con una marcada especialización en criminalidad informática.

Como explica la propia Instrucción, esta necesidad surge al haberse detectado un progresivo aumento en el número de investigaciones criminales vinculadas a la utilización de las nuevas tecnologías y más específicamente de internet, como red de redes. Es un hecho cierto que la generalización de estos instrumentos en el desarrollo de las relaciones económicas y sociales ha ido determinando la aparición de nuevas formas de criminalidad y posibilitando también dinámicas y mecanismos, hasta ahora no conocidos, en la comisión de conductas ilícitas de carácter más tradicional[169].

---

[168] Real Decreto 62/2015, de 6 de febrero, por el que se amplía la plantilla orgánica del Ministerio Fiscal para adecuarla a las necesidades existentes. *El incremento de la actividad internacional del Ministerio Fiscal y el desarrollo de la informática en los últimos años y en consecuencia de los delitos relacionados con los mismos, exige dotar al Fiscal de Sala de Cooperación Internacional que dirige la Unidad de Cooperación Internacional de la Fiscalía General del Estado y la Red de Fiscales de Cooperación Internacional, punto central de toda la actividad internacional del Ministerio Fiscal y al Fiscal de Sala Coordinador de la Criminalidad Informática del mismo número de Fiscales adscritos que al resto de Fiscales de Sala de la Fiscalía General del Estado.*

[169] Con la finalidad precisamente de dar respuesta a esta situación, potenciando una intervención especializada en este ámbito, el Excmo. Sr. Fiscal General del Estado, en Decreto dictado el 17 de abril del año 2007, otorgó delegación expresa en un Fiscal de Sala de la primera Categoría *para la dirección y coordinación de las funciones del Ministerio Fiscal en materia de delincuencia informática, facultándole para coordinar a los Fiscales que despachen tales asuntos en las distintas Fiscalías, impartiendo las instrucciones oportunas, establecer relación con las unidades policiales es especializadas en esta materia, así como para ejercer las demás funciones que considere convenientes en orden a dicha finalidad, en los términos prevenidos en la Instrucción 11/2005.* En el fundamento de la Instrucción

La Instrucción 2/2011 establece un catálogo inicial de delitos a los que se extiende el marco competencial del área de criminalidad informática, abierto a la posibilidad de hacerse extensivo a otras conductas cuando su análisis y valoración demande conocimientos específicos que hagan aconsejable su asignación a quienes integren este área de actividad del Ministerio Fiscal.

1.1 Fiscal de Sala Coordinador para la Criminalidad Informática.

La especialización se materializa mediante la creación[170] de esta figura al que se asignan las siguientes funciones[171]:

"1.- Practicar las diligencias a que se refiere el artículo cinco del Estatuto Orgánico del Ministerio Fiscal e intervenir directamente, o a través de instrucciones, en aquellos procesos penales de especial trascendencia apreciada por el Fiscal General del Estado, referentes a hechos delictivos relacionados con la Criminalidad Informática.

2.-Supervisar y coordinar la actividad de las secciones de Criminalidad Informática y recabar informes de las mismas, dando conocimiento al Fiscal Jefe del órgano del Ministerio Fiscal en que se integran.

3.- Coordinar los criterios de actuación de las distintas Fiscalías en materia de criminalidad informática, para lo cual podrá proponer al Fiscal General la emisión de

---

2/2011 de la Fiscalía General del Estado, "Sobre el Fiscal de Sala de Criminalidad Informática y las Secciones de criminalidad informática de las fiscalías".

[170] Por Real Decreto 1735/2010 de 23 de diciembre por el que se estableció la plantilla orgánica del Ministerio Fiscal para el año 2011, se creó la plaza de Fiscal de Sala Coordinador en materia de Delincuencia Informática, con la finalidad de potenciar la especialización del Ministerio Fiscal en esta materia y favorecer, aún más, la unificación de criterios de actuación en un área en la que el ritmo vertiginoso de los avances tecnológicos y la cada vez mayor utilización por parte de los ciudadanos de estos medios de comunicación interpersonal, plantea cada día a los Juristas y en concreto a los integrantes de esta Institución nuevas cuestiones que deben ser atendidas en el correcto ejercicio de las funciones que al Ministerio Fiscal corresponde desempeñar.

[171] *Vid.* artículo 20 apartados 1 y 2 de la norma estatutaria se asignan al Fiscal de Sala Coordinador para la Criminalidad Informática las siguientes funciones.

las correspondientes Instrucciones y reunir cuando proceda a los Fiscales integrantes de las secciones especializadas.

4.- Elaborar anualmente y presentar al Fiscal General del Estado un informe sobre los procedimientos seguidos y actuaciones practicadas por el Ministerio Fiscal en materia de criminalidad informática que será incorporado a la Memoria anual presentada por el Fiscal General del Estado"[172].

1.2 Las Secciones de Criminalidad Informática de las Fiscalías.

Mediante dichas secciones se articula una red de servicios territoriales de ámbito provincial integrados por uno o más Fiscales dependiendo del volumen de trabajo. Su

[172] "*Además de estas funciones, expresamente previstas en la norma estatutaria, corresponden también al Fiscal de Sala de Criminalidad Informática las atribuciones que a continuación se detallan y que son inherentes al ejercicio de su función, en términos similares a los establecidos con carácter general para los Fiscales de Sala Delegados y Coordinadores de especialidades en la Instrucción 11/2005 y en las restantes Instrucciones de la Fiscalía General del Estado dictadas hasta el momento, en relación con las distintas especialidades.*

-Coordinar la intervención del Ministerio Fiscal en las investigaciones relativas a hechos comprendidos en el marco de actuación de la especialidad cuando afecten al territorio de más de una Fiscalía provincial y revistan especial complejidad o trascendencia. Con dicha finalidad mantendrá contacto permanente con los responsables de las unidades de policía judicial de ámbito nacional o autonómico dedicadas específicamente a esta materia, coordinando las instrucciones de carácter general que se impartan a las mismas en los términos previstos en la Instrucción 1/2008 de la Fiscalía General del Estado sobre dirección por el Ministerio Fiscal de las actuaciones de la Policía Judicial.

En el ejercicio de esta función el Fiscal de Sala Coordinador de Criminalidad Informática facilitará el contacto de los Fiscales especialistas con las unidades policiales del respectivo territorio y cuidará se mantengan debidamente informados los Fiscales Superiores y los Fiscales Jefes de los correspondientes órganos del Ministerio Fiscal.

-Mantener contacto con las autoridades administrativas con competencia en esta materia para resolver las cuestiones generales que, relacionadas con su función, puedan ir planteándose. Apoyar y facilitar, a su vez, la comunicación directa que los Fiscales especialistas deban establecer con las dichas autoridades en sus respectivos territorios.

-Promover la organización y celebración de actividades formativas, cursos, jornadas de especialistas o seminarios de especialización relacionados con la Criminalidad Informática y colaborar con la Secretaría Técnica en la determinación de criterios para la formación de Fiscales especialistas, dentro del marco de los planes de formación inicial y continuada de la Carrera Fiscal.

-Impulsar y participar en la adopción de Protocolos y Convenios de coordinación y colaboración con aquellos organismos e Instituciones implicados en la prevención, investigación y persecución de los comportamientos ilícitos relativos a esta materia". Instrucción 2/2011 de la Fiscalía General del Estado, antes citada.

dimensión y estructura interna es flexible para poder adaptarse a la plantilla, el volumen de actividad y las necesidades de cada uno de los órganos del Ministerio Fiscal. La adscripción de Fiscales de la plantilla a la sección se realizará de acuerdo con lo que establece el propio Estatuto y no implica exclusividad. La dirección de estas secciones se encomienda a un Delegado Provincial[173]. Tanto el Delegado de la especialidad como los Fiscales especialistas adscritos a la sección se encuentran bajo la dependencia jerárquica del Fiscal Jefe respectivo.

Los Fiscales encargados del servicio, en función del número de procedimientos existentes en cada territorio, intervienen directamente en los expedientes o procedimientos por ciberdelitos y/o coordinan la actuación de los restantes fiscales en relación con ello. En todo caso realizan un control directo o indirecto sobre los procedimientos de esta naturaleza. La actuación de las secciones de criminalidad informática debe estar orientada a favorecer y potenciar la necesaria colaboración y coordinación con los restantes ámbitos de actividad del Ministerio Fiscal[174].

---

[173] Instrucción 2/2011 de la Fiscalía General del Estado, antes citada. "*el sistema de nombramiento del Fiscal Delegado Provincial de la especialidad, sea o no Fiscal Decano, se efectuará mediante resolución, en forma de Decreto, dictada por el Fiscal General del Estado, a propuesta del Fiscal Jefe Provincial respectivo y con audiencia del Fiscal de Sala Coordinador, previa convocatoria entre los Fiscales de la plantilla correspondiente. A dichos efectos deberán seguirse las directrices fijadas por la Inspección Fiscal en la Instrucción dictada en el año 2008 sobre procedimiento a seguir para el nombramiento en las Fiscalías territoriales de Fiscales especialistas y Fiscales Delegados de las Fiscalías Especiales".*

[174] Según la Instrucción 2/2011 de la Fiscalía General del Estado, corresponden a las secciones de criminalidad informática las siguientes funciones:
- Velar por el cumplimiento de los criterios y pautas de actuación establecidos en materia de criminalidad informática por la Fiscalía General del Estado, facilitando a dicho fin el apoyo y colaboración necesarios a los restantes integrantes de la Fiscalía y a las secciones correspondientes a otras áreas de especialización asumiendo, en los casos en los que el Fiscal Jefe lo delegue el visado de los escritos de acusación relativos a esta materia.
- Despachar e intervenir, previa determinación del Fiscal Jefe, en los procedimientos judiciales más importantes o de mayor complejidad de los comprendidos en el catálogo relacionado en el apartado II de esta Instrucción y en todo caso en los cometidos por una organización criminal, así como en las diligencias de investigación que se incoen por hechos de esta naturaleza.
- Procurar el adecuado control estadístico de los procedimientos judiciales y/o diligencias de investigación penal que se tramiten en el ámbito territorial de su competencia por los delitos anteriormente relacionados, proponiendo a tal fin al Fiscal Jefe Provincial y en su caso a los Fiscales Jefes de Área las medidas adecuadas para mantener actualizada dicha información y asumiendo las funciones que al respecto se le encomienden.
- Informar al Fiscal de Sala Coordinador de Criminalidad Informática, previo conocimiento del Fiscal Jefe respectivo, de las diligencias o procedimientos de especial trascendencia que se tramiten en el territorio provincial y de aquellos que por sus características hagan necesaria o conveniente la coordinación con otros órganos territoriales del Ministerio Fiscal.
- Participar activamente, prestando la colaboración y apoyo necesario, con conocimiento del Fiscal Jefe, en las actuaciones que, dirigidas por el Fiscal de Sala, se lleven a efecto para coordinar investigaciones

La actuación en red de estos servicios garantiza y potencia la unidad de criterio y la coordinación de aquellas investigaciones, muy frecuentes en este tipo de actuaciones, relativas a hechos que producen efectos en diversos lugares del territorio nacional. Por último, la apuesta por la especialización del Ministerio Fiscal esta siendo acompañada de actividades formativas encaminadas a hacer posible una mejor capacitación en este ámbito, con un nivel mayor de especialización respecto de los Fiscales que intervienen específicamente en las investigaciones por este tipo de actividades ilícitas y de carácter más genérico para los restantes miembros de la Fiscalía.

2. FUERZAS Y CUERPOS DE SEGURIDAD DEL ESTADO ESPECIALIZADAS EN LA LUCHA CONTRA LOS CIBERDELITOS.

Dentro de los Cuerpos y Fuerzas de Seguridad del Estado encargados de prevenir y reprimir la ciberdelincuencia existen distintas unidades especializadas tanto de ámbito estatal (en el Cuerpo Nacional de Policía y en la Guardia Civil) como autonómico (en la Ertzaina o en los Mossos d'Esquadra).

---

por hechos relacionados con la criminalidad informática que afecten al territorio de más de una Fiscalía Provincial.
- Remitir al Fiscal de Sala Coordinador la información que específicamente demande sobre diligencias o procedimientos concretos y la que con carácter general se determine, respecto de la totalidad de los expedientes relativos a criminalidad informática, por decisión del Fiscal de Sala Coordinador o por acuerdo adoptado en las reuniones de Fiscales especialistas que periódicamente se celebren.
- Organizar bajo la superior dirección del Fiscal Jefe el funcionamiento de la propia sección y sus relaciones con otras secciones y/o áreas de actuación de la Fiscalía, trasladando al mismo las necesidades, propuestas o sugerencias que se consideren oportunas para la adecuada prestación del servicio y dando cuanta de las cuestiones esenciales en relación con ello al Fiscal de Sala Coordinador.
- Elaborar anualmente un informe sobre la actividad desarrollada, los datos estadísticos disponibles, los problemas jurídicos detectados y cuantas sugerencias se consideren oportunas sobre cuestiones organizativas y/o problemas técnico-jurídicos detectados en el ámbito de actuación de la sección, dando traslado del mismo al Fiscal Jefe respectivo y al Fiscal de Sala Coordinador a los efectos de la elaboración de la correspondiente Memoria.
- Mantener las relaciones de colaboración oportunas con las unidades especializadas de las Fuerzas y Cuerpos de Seguridad del Estado ó, en su caso, de las Policías Autonómicas para garantizar la eficacia exigible en las investigaciones sobre hechos ilícitos relacionados con la criminalidad informática.

2.1 Unidad de Investigación Tecnológica del Cuerpo Nacional de Policía (UIT).

Encargada de la prevención y represión de los delitos tecnológicos como unidad central con competencia en todo el territorio nacional, así como en todo lo relativo a la colaboración internacional, formación y apoyo técnico a otras unidades[175].

Esta Unidad está compuesta por la Brigada central de Investigación Tecnológica[176] y Brigada central de Seguridad Informática. También cuenta el Cuerpo Nacional de Policía con unidades territoriales periféricas para la prevención y represión de los delitos tecnológicos en sus respectivas demarcaciones policiales[177].

De otra parte, hay que destacar los equipos conjuntos de investigación penal[178] en el ámbito de la Unión Europea en los que ha participado la policía y el Ministerio Fiscal, así como las ciberpatrullas con policías de otros países[179].

---

[175] http://www.policia.es/org_central/judicial/udef/bit_actuaciones.html 14/10/2015 a las 18.00 horas. Unidad de Investigación Tecnológica
Asume la investigación y persecución de las actividades delictivas que impliquen la utilización de las tecnologías de la información y las comunicaciones (TIC) y el ciberdelito de ámbito nacional y transnacional, relacionadas con el patrimonio, el consumo, la protección al menor, la pornografía infantil, delitos contra la libertad sexual, contra el honor y la intimidad, redes sociales, fraudes, propiedad intelectual e industrial y seguridad lógica. Actuará como Centro de Prevención y Respuesta E-Crime del Cuerpo Nacional de Policía. De esta Unidad dependerán:

- La Brigada Central de Investigación Tecnológica, a la que corresponde la investigación de las actividades delictivas relacionadas con la protección de los menores, la intimidad, la propiedad intelectual e industrial y los fraudes en las telecomunicaciones.
- La Brigada Central de Seguridad Informática la que corresponde la investigación de las actividades delictivas que afecten a la seguridad lógica y a los fraudes.

[176] La Brigada central de Investigación Tecnológica está compuesta a su vez por tres secciones: una sección de lucha contra la explotación sexual infantil en internet cuyo cometido principal es la investigación de delitos contra menores en internet; una sección de Redes dedicada a la investigación de delitos cometidos en el ámbito de las Redes Sociales, así como investigaciones en Fuentes Abiertas y delitos de amenazas, calumnias e injurias cometidos en internet y una sección técnica que presta apoyo técnico a la propia unidad y a otras unidades operativas y realiza tareas tanto de formación como de I+D (investigación y Desarrollo) ataques, intrusiones, uso delictivo de malware, etc. y otra de Fraudes online que investiga una amplia variedad de fraudes cometidos a través del uso de las nuevas tecnologías. Cada una de las mencionadas secciones está compuesta por grupos especializados en las diferentes áreas de la delincuencia informática.

[177] En su página web (http://www.policia.es/org_central/judicial/udef/bit_alertas.html) se puede encontrar información de todo tipo acerca de sus intervenciones, acciones, etc., así como interponer denuncias si se ha sido objeto de algún ciberdelito.

[178] *Vid*. infra. Equipos Conjuntos de Investigación. Se crearon al amparo de la Ley 11/2003, de 21 de mayo. La eficacia de los Equipos Conjuntos de Investigación Penal en el ámbito de la Unión Europea, es que pueden funcionar sin necesidad de tramitar comisiones rogatorias.

2.2 Grupo de Delitos Telemáticos de la Guardia Civil (GDT)[180].

Creado para investigar todos aquellos delitos cometidos a través de Internet. Cuenta con un diseño estratégico que contempla este tipo de amenaza. Dispone de una estructura para luchar contra los hechos delictivos cometidos en la red que consiste en diferenciar lo que serían Unidades de Seguridad Ciudadana, como policía judicial genérica, y encargadas de prestar los servicios de atención al ciudadano, de las Unidades Policía Judicial específica. Mientras que las primeras son las llamadas a recibir la inmensa mayoría de las denuncias, ya que son el primer contacto con el que cuentan las víctimas de ciberdelitos, sobre las Unidades de Policía Judicial recae la responsabilidad de investigar aquellos hechos delictivos que, por su especial dificultad o por la sensibilidad del bien jurídico protegido, requieren una formación específica.

Las Unidades Orgánicas de Policía Judicial, cuentan con una Sección de Investigación que aborda los casos más graves. Su estructura se conforma tratando de contar especialización delictiva[181]. Los denominados delitos tecnológicos o relativas a la ciberdelincuencia se investigan desde dos frentes distintos:

---

[179] España, a través de la Unidad de Investigación Tecnológica del Cuerpo Nacional de Policía, es co-lider en la subprioridad de ciberataques del proyecto EMPACT de Europol. En el plan operativo de dicha subprioridad existe una actividad (5.1) relativa a las ciberpatrullas la cual es co-liderada por España junto con Alemania.

[180] https://www.gdt.guardiacivil.es/webgdt/home_alerta.php 14/10/2015 a las 18.14 horas.
Su origen se remonta al año 1.996, cuando se constituyó el Grupo de Delitos Informáticos (GDI) para atender a las pocas denuncias que había entonces por los llamados delitos informáticos. Su buen hacer y el crecimiento exponencial de usuarios de la red, propiciaron el crecimiento del grupo, que pasó a llamarse Departamento de Delitos de Alta Tecnología (DDAT), asumiendo como nueva competencia el fraude en el sector de las telecomunicaciones.
Con la socialización de Internet y el crecimiento de los hechos delictivos, se amplía el abanico de competencias de investigación, que alcanza a todas aquellas conductas delictivas realizadas a través de los sistemas de información o contra éstos, lo que se conoce popularmente como el cibercrimen. El departamento cambia de nombre por el actual, Grupo de Delitos Telemáticos (GDT). Estos cambios se acompañaron de la creación de los Equipos de Investigación Tecnológica (EDITE,s) en cada uno de las provincias de España. El esfuerzo principal del GDT y de los EDITE,s ha sido, desde su creación, la investigación de la delincuencia que se vale de las redes y sistemas de información para su comisión. También cabe destacar los esfuerzos que realizan para fomentar un uso seguro de las nuevas tecnologías, consciente de que a la larga este esfuerzo ayudará a minimizar el impacto de la delincuencia.

[181] También, en este ámbito, dentro de la Unidad Técnica de Policía Judicial, se dispone de una Sección de Análisis Criminal que se encarga de la elaboración de la inteligencia relativa a la delincuencia tecnológica, canaliza las informaciones e intercambios de datos, tanto en el ámbito nacional como internacional, dirige la participación en los foros que se establecen al respecto (nacionales o internacionales), realiza un seguimiento de esta casuística, coordina las investigaciones de las Unidades cuando es preciso, se encarga de materializar la formación y actualización técnica y operativa de los Especialistas de las Unidades de Policía Judicial de la Guardia Civil y centraliza las relaciones institucionales que, en el ámbito de Policía Judicial, tengan relación con los delitos telemáticos.

1º) Desde el área de delitos relacionados con las personas, donde se encuentran los EMUMES (Equipos Mujer-Menor) encargados de realizar las investigaciones relacionadas con la pornografía infantil y los delitos cometidos contra los menores (*grooming, ciberbulling* etc). En este ámbito, además de investigar el ciberdelito, el objetivo último de estas actuaciones es lograr la identificación de los menores víctimas, y en el caso de los autores menores, se busca también que sean investigados por personal especializado.

2º) Desde el área de los delitos relacionados con el patrimonio, donde se engloban los EDITES (Equipos de Investigación Tecnológica), responsables de hacer frente a toda delincuencia que se sirva para su comisión de los elementos tecnológicos, a excepción de los relativos a menores y los que por su dificultades técnicas necesiten de una preparación especializada

En el ámbito nacional, y también como escalón operativo, es el *Grupo de Delitos Tecnológicos* (GDT) de la Unidad Central Operativa (UCO) el que desarrolla la investigación de este tipo de hechos cuando revisten especial dificultad, complejidad o trascendencia. Igualmente, presta los apoyos técnico-operativos requeridos por las Unidades territoriales antes mencionadas.

Y también como parte de la estructura central, el Servicio de Criminalística del Departamento de Electrónica e Informática tiene como cometido la realización de peritajes informáticos y digitales así como el análisis forense de los dispositivos e indicios electrónicos, intervenidos en actuaciones de las Unidades operativas y que servirán *a posteriori*, como prueba ante los tribunales de justicia.

En último lugar, la Jefatura de Información posee un área dedicada en exclusiva a combatir el ciberterrorismo en todas sus vertientes, y cualquier grupo que pueda considerarse como desestabilizador para la seguridad nacional.

También cabe señalar que desde un punto de vista operativo se trabaja específicamente en reforzar la coordinación entre las unidades policiales especializadas en este tipo de investigaciones y los servicios territoriales de criminalidad informática del Ministerio Fiscal. Con ese mismo objetivo se han constituido en la Unidad Central

de Criminalidad Informática, sendas oficinas de enlace con el Cuerpo Nacional de Policía y la Guardia Civil justamente para reforzar e impulsar la transmisión ágil y eficaz de la información y en definitiva la actuación coordinada de las distintas fuerzas policiales con el Ministerio Fiscal en esta materia.

También debe destacarse en el ámbito europeo la participación de la Guardia Civil en ciberpatrullas y en Equipos Conjuntos de Investigación[182], incluso rastrean o "patrullan" por internet mediante programas informáticos específicos para detectar ciberdelitos como la piratería informática o la distribución de pornografía infantil.

3. LOS EQUIPOS CONJUNTOS DE INVESTIGACIÓN (JIT).

De gran importancia para la investigación del ciberdelito por su carácter transnacional son los Equipos Conjuntos de Investigación (en adelante, JIT)[183] si bien, en España es un instrumento infrautilizado. Así, desde un punto de vista numérico, si se compara a modo de ejemplo con otros países de nuestro entorno, España tenía en el año 2016 nueve equipos conjuntos de investigación mientras que en Finlandia estaban operando cincuenta y nueve equipos[184].

La Decisión Marco 2002/465/JAI del Consejo, de 13 de junio de 2002[185], fue la que estableció la posibilidad de que los Estados miembros constituyeran equipos

[182] Equipo Conjunto de Investigación creado por Eurojust en la "*Operación "Eurymus*", en la que participaron junto con Reino Unido, Eslovenia, Finlandia y Rumanía.

[183] Acrónimo del Inglés *Joint Investigation Team*.

[184] VILLODRE LÓPEZ, J. "*Los Equipos Conjuntos de Investigación (JIT)*". Ponencia presentada el día 20 de abril de 2016 en las IV Jornadas de Derecho Procesal organizadas por la 7ª Zona de la Guardia Civil de Catalunya, Sobre Cooperación Judicial Penal. Villodre López, J. Es el Magistrado del Punto de Contacto de la Red Europea de Equipos Conjuntos.

[185] El origen de esta Decisión Marco se debe a la reunión de Tampere en 1999, donde los Estados miembros se comprometieron a la creación, con la mayor brevedad posible, de equipos conjuntos de investigación con el fin de luchar contra el tráfico de drogas, la trata de seres humanos y el terrorismo. El Convenio relativo a la asistencia judicial en materia penal que se adoptó en mayo de 2000 preveía la creación de equipos conjuntos de investigación. No obstante, con motivo de la tardanza de los Estados miembros para ratificar el Convenio, en junio de 2002 el Consejo adoptó la Decisión marco sobre equipos conjuntos de investigación que los Estados miembros debían aplicar antes del 1 de enero de 2003.

conjuntos de investigación cuando se precise una acción coordinada y concertada[186]. Estos JIT deberían tener un objetivo preciso y una duración limitada.

En cumplimiento de esa Decisión Marco y sin esperar a su aprobación definitiva España[187], en atención a la enorme utilidad que los JIT podrían tener en la investigación frente a ETA, adelantó la regulación nacional y promulgó dos Leyes[188]:

a) La *Ley 11/2003, de 21 de mayo, reguladora de los equipos conjuntos de investigación penal en el ámbito de la Unión Europea.* Donde se define el Equipo conjunto de investigación, como el constituido por acuerdo de las autoridades competentes de dos o más Estados miembros de la Unión Europea para llevar a cabo investigaciones penales en el territorio de alguno o de todos ellos, que requieran una actuación coordinada, con un fin determinado y por un periodo limitado.

b) La *Ley Orgánica 3/2003, de 21 de mayo, complementaria de la Ley reguladora de los equipos conjuntos de investigación penal en el ámbito de la Unión Europea, por la que se establece el régimen de responsabilidad penal de los miembros destinados en dichos equipos cuando actúen en España*[189].

---

[186] En el ámbito de Naciones Unidas, el art. 19 del Convenio contra la Delincuencia Organizada Trasnacional hecho en Nueva York el 15 de noviembre de 2000 (conocido como Convenio de Palermo) prevé las investigaciones conjuntas a través de acuerdos bilaterales o multilaterales entre los países que lo suscriban o de acuerdos específicos casos concreto. De igual forma la Convención de Naciones Unidas contra la Corrupción hecha en Nueva York el 31 de octubre de 2003 (conocida como Convenio de Mérida) recoge en su artículo 49 las investigaciones conjuntas como métodos de investigación de estos delitos. También convenios bilaterales suscritos por España suelen prever esta técnica. Así lo hace el Acuerdo de Asistencia Judicial en materia penal entre la Unión Europea y los Estados Unidos celebrado en Washington el 25 de junio de 2003 en su artículo 16 ter, y el protocolo adicional de 12 de Julio de 2005 al Convenio de cooperación Colombia de 20 de mayo de 1997.

[187] "*Sin esperar a la aprobación definitiva de la Decisión Marco de 2002 pero basándose en su texto negociado en el Consejo*." Informe del consejo fiscal en relación con la problemática relativa a los Equipos Conjuntos de Investigación, Madrid 23 de julio de 2014 pág. 3.

[188] VILLODRE LÓPEZ, J. "Los Equipos Conjuntos de Investigación (…) ob. cit. Villodre López, J. sostuvo además durante la ponencia que aunque estas Leyes solo son de aplicación en el ámbito de la UE, no habría problema en constituir JIT con otros países fuera de la Unión siempre que mediara el correspondiente acuerdo Constitutivo.

[189] Informe del Consejo Fiscal en relación con la problemática relativa a los Equipos Conjuntos de Investigación, madrid 23 de julio de 2014. pág. 3.
"*Por actuar con esa urgencia y sin tener en cuenta la necesidad de adecuar la regulación europea al procedimiento penal español, la regulación española de los equipos conjuntos puede tildarse de desacertada ya que, aunque sin duda es bastante fiel a la regulación de la Decisión Marco, olvida adaptar el instrumento a la realidad de la Ley de Enjuiciamiento Criminal y a la estructura de nuestra*

Estos JIT pueden ser en función del número: bilaterales (si es entre dos Estados) o multilaterales (si son más de dos). Y según su naturaleza: Policial[190], Fiscal[191] o Judicial, dependiendo del órgano de investigación.

Además, su importancia radica en que no se precisa comisión rogatoria, lo que agiliza la practica de las diligencias de investigación que se requieran a la vez que aúna celeridad y eficacia.

La legislación que rige la práctica de esas diligencias es la del Estado en el que se actúa, por lo que en caso de practicarse fuera del territorio español, se deberá pedir que se adopten las mismas condiciones que si fueran practicadas en el marco de una investigación española.

Administración de Justicia y por ello se están produciendo problemas en la práctica que podrían empezar a generar reclamaciones de las partes y posibles nulidades en procedimientos judiciales".

[190] VILLODRE LÓPEZ, J. "Los Equipos Conjuntos de Investigación (JIT)". Ponencia presentada el día 20 de abril de 2016 en las IV Jornadas de Derecho Procesal organizadas por la 7ª Zona de la Guardia Civil de Catalunya, Sobre Cooperación Judicial Penal. Villodre López, J. Sostuvo que las Policías autonómicas quedaban excluidas de los JIT, pues según la normativa solo podía constituirse con Fuerzas y Cuerpos de Seguridad del Estado. No obstante, las Policías Autonómicas, en los casos en que sea necesario, pueden incluirse en el acuerdo constitutivo del JIT siempre bajo el paraguas de la Policía de ámbito nacional.

[191] En la Memoria de la Fiscalía General del Estado del año 2015, págs. 615 y 616 se destaca la participación de la Fiscalía en la llamada "*operación Eurymus"* desarrollada con el objetivo de desmantelar una organización delictiva que se valía de programas o malwares creados al efecto, para llevar a cabo intrusiones en los sistemas informáticos de distintas empresas de las que se descargaban bases de datos con información sobre tarjetas de crédito y usuario de sus clientes que después vendían a terceros para su ilícito uso.
También en la*"operación Onymous*" dirigida contra mercados clandestinos de internet en la que, tras geolocalizarse en Arenys de Mar (Barcelona) una página Web desde la que supuestamente se estaba llevando a efecto la venta de euros falsos a cambio de bitcoins, la participación del Fiscal Delegado de Barcelona, designado a tal efecto por la Fiscal de Sala, resultó decisiva para poder materializar la práctica simultánea con Europa y Estados Unidos de las diligencias de entrada y registro acordadas. En esta última operación la actuación de la Fiscalía española fue objeto de felicitación desde Eurojust.
Participación de la Fiscalía en la denominada "*operación Atelier*" dirigida contra un grupo de personas que de manera estable y estructurada utilizaban niñas menores de edad, incluso menores de 13 años, para elaboración de material pedófilo, mediante la elaboración de guiones para los posados y vídeos, selección de niñas concretas y envío de ropas para las niñas, materiales que eran enviados por el sospechoso español al intermediario en Suecia, quien a su vez lo enviaba a fotógrafos en República Checa. La colaboración de los tres países fue esencial para detención de los sospechosos y para la realización de las diligencias de entradas y registros simultáneas, lo que permitió, sin que existiera destrucción de evidencias electrónicas, la incautación de los dispositivos informáticos donde se almacenaba el material pedófilo.
Uno de los últimos en los que ha participado la Unidad de Investigación Tecnológica de la policía corresponde a la "*Op. Alfonsos"* iniciada como consecuencia de información remitida por la fiscalía sueca a la española, acerca de la intervención, en un grupo organizado internacional, de producción y venta de pornografía infantil, de un sospechoso español que ya había sido condenado en España, en 2013, por su participación en hechos similares ("*Operación Koala"*, año 2007) en el proceso de producción y compraventa de pornografía infantil.

Para la creación de los JIT es necesario la adopción de un acuerdo constitutivo que deberá contener las especificaciones del artículo 5 de la Ley 3/2003[192]. Uno de los problemas de la regulación española es el de la autoridad competente para la constitución del equipo, pues se requiere autorización previa de la Autoridad Nacional para su constitución[193]. El art. 3 de la Ley 11/2003 establece que autoridad competente será:

a) La Audiencia Nacional, cuando la investigación recaiga sobre los delitos cuyo enjuiciamiento corresponda a dicho órgano jurisdiccional y participen en el equipo miembros de la carrera judicial o fiscal[194].

b) El Ministerio de Justicia, cuando la investigación recaiga sobre los delitos para cuyo enjuiciamiento no resulte competente la Audiencia Nacional y participen en el equipo miembros de las carreras judicial o fiscal[195].

---

[192] El Diario Oficial de la Unión Europea de 19 de enero de 2017 publica la resolución del Consejo 2017/C 18/01 relativa a un modelo de Acuerdo por el que se crea un Equipo Conjunto de Investigación. http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32017G0119(01)&from=ES
También en el prontuario se puede obtener modelos sobre acuerdos de constitución y la Guía Práctica JIT.

[193] La Ley carece de cualquier referencia a la regulación procesal de la actuación de los equipos, su documentación, su incorporación al expediente judicial, la presentación de las pruebas, la posibilidad de compartir las pruebas, la posible participación de investigadores extranjeros como elemento probatorio, la valoración que deba darse a la valoración hecha de una prueba en otro Estado. No se hace referencia tampoco a la participación de las partes en los equipos conjuntos y aunque parece razonable que solo puedan existir equipos conjuntos mientras las diligencias se encuentran declaradas secretas, nada se dice en la norma y ya se están planteando las consecuencias de la negativa a la participación de los abogados defensores en diligencias practicadas en el ámbito del equipo.

[194] Informe del Consejo Fiscal en relación con la problemática relativa a los Equipos Conjuntos de Investigación, Madrid 23 de julio de 2014. pág. 5.
"Llama la atención es la mención a la "Audiencia Nacional" como autoridad competente, una mención que tiene una significación ininteligible en el marco jurídico, orgánico y procesal lo que es fuente de continuos problemas interpretativos a la hora de concretar el órgano competente dentro de la misma.
En ocasiones se ha defendido que la referencia debe considerarse hecha a la Sala de Gobierno de la Audiencia Nacional en tanto que se interpreta que el acuerdo de constitución no es una tarea propiamente jurisdiccional. Por el contrario, otros sostienen que la referencia a la Audiencia Nacional debe entenderse hecha a la Sala de lo Penal de dicho órgano".

[195] Informe del Consejo Fiscal en relación con la problemática relativa a los Equipos Conjuntos de Investigación, Madrid 23 de julio de 2014. pág. 6.
"La segunda cuestión que se plantea ante esta regulación es que no se explica ni puede justificarse constitucionalmente el motivo de una diferente atribución de competencias que otorga plena autonomía a la Audiencia Nacional y somete al resto de los órganos competentes al criterio y voluntad del Ministerio de Justicia. Es evidente que la jurisdicción de unos y otros órganos judiciales es idéntica y debe ser completa sobre los asuntos de su competencia. La distribución de competencias entre órganos territoriales y Audiencia Nacional se realiza en atención al tipo de delito y al lugar o lugares donde se cometen, pero las atribuciones para la actuación en relación con los delitos que recaen en sus

c) El Ministerio de Interior, a través de la Secretaría de Estado de Seguridad, en todos los supuestos en que no participen miembros de las carreras judicial o fiscal.

No se entiende que los jueces, a excepción de los de la Audiencia Nacional, tengan que solicitar para la creación de dichos equipos la autorización del Ministerio de Justicia, cuando para las comisiones rogatorias no es necesario. Ello es así porque la Ley parte de un paradigma erróneo y es que concibe a los JIT como acuerdos entre Estados y no entre Autoridades Judiciales. En este sentido está pendiente de resolver una cuestión de inconstitucionalidad de esta ley, planteada por la Audiencia Provincial de Málaga en el año 2015[196], que considera que la previa y necesaria autorización del Ministerio de Justicia para la constitución o ampliación de los JIT puede ser contraria la artículo 117 de la Constitución Española, al suponer una incidencia directa en la labor jurisdiccional en la medida en que otorga a la autoridad administrativa competencias importantes dentro del procedimiento penal.

respectivas competencias son las mismas y no hay en la Ley Orgánica del Poder Judicial limitación alguna que permita un tratamiento diferente en relación con los ECI como instrumento de cooperación internacional. Parece por tanto injustificada e injustificable la limitación y diferencia que la Ley de Equipos Conjuntos realiza de la jurisdicción y competencias de los órganos judiciales y las Fiscalías que no actúan en el ámbito de los delitos que competen a la Audiencia Nacional.

[196] Auto 940/15 de la Audiencia Provincial de Málaga (sección 9ª) de 18 de noviembre de 2015, de planteamiento de cuestión de inconstitucionalidad.
Se plantea la cuestión de la posible inconstitucionalidad de los arts. 3 párrafo segundo y 9 párrafo primero de la Ley de equipos conjuntos de investigación, conforme a lo dispuesto en el art 35.2 de la LOTC, en base a la posible vulneración de estos preceptos de lo dispuesto en el art 117 de la CE en la medida en que al poder un órgano administrativo deshacer a su antojo los equipos conjuntos de investigación, se deja en manos de un órgano no jurisdiccional la dirección y control de la investigación penal, si la investigación no se lleva a cabo por la Audiencia Nacional, supuesto en el que si se contempla que la dirección de los equipos de investigación corresponde a la autoridad judicial.
Concretamente los arts. de cuya constitucionalidad se duda son los siguientes el art. 3 en su párrafo segundo, es decir en el apartado correspondiente a los procedimientos por delitos cuyo conocimiento no correspondan a la Audiencia Nacional y el párrafo primero del art. 9 en relación con el anterior en cuanto que se atribuye la posibilidad de ampliación de la investigación a la autoridad administrativa en los mismos términos.

4. LAS EMPRESAS PROVEEDORAS DE INTERNET (ISP).

La colaboración de los proveedores de Internet *(Internet service provider* o ISP) es esencial en la investigación de los delitos cometidos utilizando las Tecnologías de Información y Comunicaciones (TIC), al ser éstos quienes disponen y pueden proporcionar los datos de cualquier interacción en el ciberespacio.

Dentro de los ISP hay que distinguir entre los proveedores de acceso y los proveedores de servicios. Los primeros son las compañías que proporcionan el acceso a internet, que normalmente suelen ser operadoras de telecomunicaciones (como es el caso de las empresas Movistar, Orange, Vodafone etc.), mientras que los segundos son aquellos que proporcionan ciertos servicios de uso común como el correo electrónico (Hotmail, Gmail), redes sociales (Facebook, Twitter), almacenamiento de archivos (Dropbox, Googledrive), publicación de videos y fotos (Youtube, Panoramio, flickr), o mensajerías (whatsApp, Line) etc.

Obviamente, en la consecución probatoria es crucial el papel de las empresas de telecomunicaciones y servidoras de internet en su colaboración con la Justicia. Estas empresas han de tratar de compatibilizar el desarrollo de la libertad de expresión, comercio, conocimientos y comunicaciones que potencia internet a través de sus múltiples mecanismos y posibilidades, con la exclusión del mayor número de contenidos ilícitos posible[197].

Es indispensable contar con la cooperación de estos operadores de telecomunicaciones y los proveedores de servicios de internet, dado que poseen la información necesaria sobre los abonados y suscriptores[198]. Adviértase que poseen datos sobre el tráfico de comunicaciones anteriores generados por un equipo que registra

[197] *Vid.* STEDH (Sección 4ª) 2 diciembre 2008, caso K.U. contra Finlandia (art. 8) en la que se condena a este Estado por no tener normativa que obligue a los ISP a entregar los datos requeridos judicialmente para la investigación de los ciberdelitos. Se trataba de un anuncio de naturaleza sexual aparecido en internet, cuyo protagonista era un menor de 12 años, la legislación de Finlandia no permitía conocer a través del proveedor la identidad de quien lo colgó por lo que se consideró que el Estado incumplió su obligación de proteger a la víctma, al no poder llevar a cabo acciones para identificar y procesar a su autor.

[198] En terminología de la Sociedad de la Información se suele distinguir entre abonado a un servicio de telecomunicaciones y suscriptor a un servicio de Internet.

detalles, en particular la hora, la duración y la fecha de cualquier comunicación, las partes que la sostuvieron o el tipo de servicio o actividad. Estos datos se conservan por lo general durante un período de tiempo limitado según las necesidades comerciales del operador o proveedor y los requisitos legales o comerciales para la protección de la esfera privada.

Los ISP mantienen la obligación de conservar estos datos asociados a la comunicación y cederlos siempre y cuando medie autorización judicial, en virtud de la Ley 25/2007 de conservación de datos y la LECrim, incurriendo en responsabilidad en caso de incumplimiento.

Por concretar, cabe establecer cuatro momentos distintos en los que la LECrim impone el deber de colaboración a las ISP:

1) En la conservación y cesión de datos (art. 588 ter j LECrim).

Los sujetos pasivos destinatarios de la obligación de conservar los datos de la Ley 25/2007, son los proveedores de servicios de internet y operadoras que prestan servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones. Para saber con precisión quienes son los sujetos obligados sólo hay que acudir al Registro de Operadores[199] dependiente del Ministerio de Industria, Energía y Turismo a través de la Comisión Nacional de los Mercados y la Competencia, regulado en el artículo 7 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones[200]. La LECrim amplía esta obligación a los que se conserven por propia iniciativa por motivos comerciales o de otra índole.

[199] https://telecos.cnmc.es/registro-de-operadores

[200] En este registro no están, y por tanto no les alcanza la obligación de retener los datos de tráfico, las denominadas plataformas OTT (over the top), que incluyen nombres tan conocidos como WhatsApp, Skype o Telegram, existiendo un conflicto abierto entre las operadoras tradicionales y estas plataformas con varios frentes, entre ellos la exigencia de que se sometan a la misma normativa que las operadoras, ya que en muchos casos prestan servicios similares y además se aprovechan sin ningún tipo de contraprestación de la infraestructura que costea y mantiene la operadora que suministra el acceso a internet. Ni tampoco están los servidores web de correo electrónico (Yahoo, Gmail, Microsoft) que tiene su sede fuera de España, aunque en la práctica están proporcionando los datos que se les solicitan por los juzgados en investigaciones penales, si bien el período de conservación de los datos depende de la política de cada servidor.

Además de las responsabilidades penales que pudieran derivarse del incumplimiento de la obligación de conservación y cesión de datos a los agentes facultados, se establece también una responsabilidad administrativa[201].

2) En la intervención de las comunicaciones (artículo 588 ter e). Se establece un deber de colaboración y de secreto por parte de los operadores cuyo incumplimiento será constitutivo de un delito de desobediencia.

El sujeto obligado se amplía con respecto a los destinatarios de la obligación de conservar los datos previstos en la Ley 25/2007. Con arreglo al artículo 588 ter e LECrim, tan obligada queda una compañía de telecomunicaciones tradicional, que suministre acceso a la red telefónica, una compañía de videojuegos *on line* o cualquier persona que facilite la comunicación. Todas deberán favorecer a los agentes facultados la intervención de las comunicaciones entre aquellos usuarios que queden afectados por una orden judicial. Otra cosa será que dicha intervención sea técnicamente factible. O que las compañías extranjeras que facilitan estos servicios se consideren vinculadas por la legislación española[202].

3) La orden de conservación de datos del art. 588 octies LECrim. Tiene por objeto datos informáticos vinculados a investigaciones concretas, por lo que ha de solicitarse en cada supuesto en que se estime necesaria la preservación de determinada información incluida en un sistema informático o de almacenamiento de datos[203]. Se impone esta obligación reforzada con el delito de desobediencia en caso de incumplimiento, a "cualquier persona física o jurídica", extendiéndose así no sólo a los operadores de telecomunicaciones, sino a cualquier otro sujeto que almacene los datos o informaciones, como pueden ser en un momento dado, los particulares que puedan

---

[201]Así, se regula un régimen de infracciones y sanciones previsto en el artículo 10 de Ley 25/2007 de conservación de datos, que remite al régimen sancionador establecido en la Ley General de Telecomunicaciones, correspondiendo la competencia sancionadora al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información, o a la Agencia Española de Protección de datos, según el tipo de infracción que se cometa.

[202] BERMÚDEZ GONZÁLEZ, J. Deber de colaboración de particulares en LECrim. Ponencia presentada en el curso de Formación de Fiscales "Uso de las nuevas tecnologías y nuevas formas de delincuencia" que se celebró en el Centro de Estudios Jurídicos los días 27 al 28 de octubre de 2016. pág. 7. http://www.cej-mjusticia.es.

[203] TEJADA DE LA FUENTE, E. La retención obligatoria de datos de tráfico de las comunicaciones electrónicas y telemáticas (…) ob. cit. págs. 340 y 341, resume las diferencias existentes entre esta medida y la obligación genérica de conservación de los datos de tráfico.

canalizar el tráfico de la red TOR, o aquéllos cuyos ordenadores hayan sido empleados para el acceso fraudulento a internet y cuyo examen pueda necesitarse por los investigadores[204].

4) Por último, en el registro remoto (art. 588 septies b LECrim). También quedan obligados a colaborar para la práctica de la medida y el acceso al sistema los prestadores de servicios y personas señaladas en el artículo 588 ter e y los titulares o responsables del sistema informático o base de datos objeto del registro, incurriendo en desobediencia en caso contrario.

Otra cuestión, es que los proveedores de servicios (según la Ley 34/2002 de Servicios de la Sociedad de la Información y del Comercio Electrónico) no son responsables de los contenidos que transmiten o alojan o a los que facilitan acceso, si no participan en su elaboración o no tienen conocimiento de la ilegalidad de los mismos. Son responsables si conocen su ilicitud y no actúan rápidamente para retirarlos o imposibilitar el acceso a ellos. Tienen obligación de denunciar los contenidos delictivos que detecten en sus servidores[205]. Las solicitudes de bloqueo de acceso o retiradas de contenidos o sitios web deberán ser requeridas con autorización judicial.

Nuestro ordenamiento jurídico permite la imputación de delitos a personas jurídicas por ciberdelincuencia, por lo que es posible realizar cualquier diligencia

[204] RÍOS PINTADO. J F. "La reforma Procesal. Incorporación al proceso de datos de tráfico; preservación específica de datos informáticos (arts. 588 ter j y 588 octies de la LECrim). Ponencia presentada en el curso de Formación de Fiscales "Uso de las nuevas tecnologías y nuevas formas de delincuencia" que se celebró en el Centro de Estudios Jurídicos los días 27 al 28 de octubre de 2016. http://www.cej-mjusticia.es.

[205]A medida que los pederastas abandonan las redes P2P para el intercambio de archivos pornográficos, conscientes de su vulnerabilidad, suelen acudir a medios de envío y recepción de archivos entre particulares. Los ejemplos son variopintos, desde archivos adjuntos al correo electrónico, al uso de carpetas compartidas en discos duros en la nube, a la mensajería instantánea integrada en las redes sociales. Determinadas empresas, como Microsoft o Facebook, conscientes del uso criminal de sus servicios han implementado herramientas de control preventivo del intercambio de este material, como el software PhotoDNA, que comparten las dos corporaciones mencionadas. Este programa calcula, automáticamente, el hash de todo archivo que se carga en sus servidores por parte de un usuario. Estas firmas hash son comparadas con una base de datos de la que dispone NCMEC (National Center forMissing&ExploitedChildren, Centro Nacional para Menores Desaparecidos y víctimas de Explotación), y si ofrece un resultado positivo, se pone inmediatamente en conocimiento de las autoridades.

procesal en el marco de una investigación cuando haya intervenido la empresa o haya sido utilizada para la comisión de alguno de estos delitos[206]:

1) Delitos relacionados con ordenadores y ataques contra los sistemas de información: la reforma operada por la Ley Orgánica 1/2015 añadió un nuevo artículo 197 quinquies al capítulo dedicado al "descubrimiento y revelación de secretos" del Código Penal, a fin de regular la responsabilidad de una persona jurídica en los casos de los delitos relacionados con ordenadores y sistemas de información, en particular los ataques contra los mismos[207].

2) Delitos relacionados con el contenido, en particular los relacionados con el abuso sexual de menores en línea y con la pornografía infantil[208].

---

[206]Con carácter general, señala el apartado III de la Exposición de Motivos de Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, publicada en el Boletín Oficial del Estado de 31 de marzo de 2015 que:
"La reforma lleva a cabo una mejora técnica en la regulación de la responsabilidad penal de las personas jurídicas, introducida en nuestro Ordenamiento jurídico por la Ley Orgánica 5/2010, de 22 de junio, con la finalidad de delimitar adecuadamente el contenido del "debido control", cuyo quebrantamiento permite fundamentar su responsabilidad penal. Con ello se pone fin a las dudas interpretativas que había planteado la anterior regulación, que desde algunos sectores había sido interpretada como un régimen de responsabilidad vicarial, y se asumen ciertas recomendaciones que en ese sentido habían sido realizadas por algunas organizaciones internacionales. En todo caso, el alcance de las obligaciones que conlleva ese deber de control se condiciona, de modo general, a las dimensiones de la persona jurídica."

[207]Se trata de los delitos comprendidos en los artículos 197, 197 bis y 197 ter CP. En estos casos, a la persona jurídica responsable se le impondrá la pena de multa de seis meses a dos años y se prevé que, en determinados casos los jueces y tribunales puedan asimismo imponer otras penas, que serían las siguientes (recogidas en las letras b) a g) del apartado 7 del artículo 33 del CP, a cuyo tenor:
"*b) Disolución de la persona jurídica. La disolución producirá la pérdida definitiva de su personalidad jurídica, así como la de su capacidad de actuar de cualquier modo en el tráfico jurídico, o llevar a cabo cualquier clase de actividad, aunque sea lícita.*
c) Suspensión de sus actividades por un plazo que no podrá exceder de cinco años.
d) Clausura de sus locales y establecimientos por un plazo que no podrá exceder de cinco años.
e) Prohibición de realizar en el futuro las actividades en cuyo ejercicio se haya cometido, favorecido o encubierto el delito. Esta prohibición podrá ser temporal o definitiva. Si fuere temporal, el plazo no podrá exceder de quince años.
f) Inhabilitación para obtener subvenciones y ayudas públicas, para contratar con el sector público y para gozar de beneficios e incentivos fiscales o de la Seguridad Social, por un plazo que no podrá exceder de quince años.
g) Intervención judicial para salvaguardar los derechos de los trabajadores o de los acreedores por el tiempo que se estime necesario, que no podrá exceder de cinco años".

[208]Conforme al artículo 189 bis CP, cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en este Capítulo, se le impondrán las siguientes penas:
a) Multa del triple al quíntuple del beneficio obtenido, si el delito cometido por la persona física tiene prevista una pena de prisión de más de cinco años.
b) Multa del doble al cuádruple del beneficio obtenido, si el delito cometido por la persona física tiene prevista una pena de prisión de más de dos años no incluida en el anterior inciso.

3) Delitos en que ordenadores o sistemas y tecnologías de la información fueron herramientas para delinquir u objeto principal del delito, en particular el fraude en línea y con tarjetas de pago[209].

4) Para los delitos referidos a las rúbricas "interferencia ilegal en los datos", "interferencia ilegal en los sistemas de información" e "instrumentos utilizados para cometer las infracciones", tipificados en los artículos 264 CP, 264 bis CP y 264 ter CP[210].

5) Los llamados delitos de odio[211].

Por último, el 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

---

c) Multa del doble al triple del beneficio obtenido, en el resto de los casos.
Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33 del CP, antes citado

[209]Conforme al artículo 251 bis CP cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en esta Sección, se le impondrán las siguientes penas:
a) Multa del triple al quíntuple de la cantidad defraudada, si el delito cometido por la persona física tiene prevista una pena de prisión de más de cinco años.
b) Multa del doble al cuádruple de la cantidad defraudada, en el resto de los casos. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33.

[210]El artículo 264 quater CP, se establece que cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en los tres artículos anteriores, se le impondrán las siguientes penas:
a) Multa de dos a cinco años o del quíntuplo a doce veces el valor del perjuicio causado, si resulta una cantidad superior, cuando se trate de delitos castigados con una pena de prisión de más de tres años.
b) Multa de uno a tres años o del triple a ocho veces el valor del perjuicio causado, si resulta una cantidad superior, en el resto de los casos.
Además se prevé que, atendidas las reglas establecidas en el artículo 66 bis, al que anteriormente nos hemos referido, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33.

[211]La sanción a las personas jurídicas, dispone el artículo 510 bis CP que cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en los dos artículos anteriores, se le impondrá la pena de multa de dos a cinco años. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33. En este caso será igualmente aplicable lo dispuesto en el número 3 del artículo 510 del Código Penal, es decir, que será aplicable la agravante establecida en el mismo y las penas previstas se impondrán en su mitad superior cuando los hechos se hubieran llevado a cabo a través de un medio de comunicación social, por medio de internet o mediante el uso de tecnologías de la información, de modo que, aquel se hiciera accesible a un elevado número de personas.

que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)[212], establece la obligación de las empresas que prestan servicios de la conocida como Sociedad de la Información, de comunicar a las autoridades nacionales cuando sufran un incidente relacionado con la seguridad de la información[213], por lo que con este artículo se pondrá fin al silencio de las grandes compañías, que no daban cuenta de estos incidentes para evitarse perjuicios en su reputación con el consiguiente perjuicio para los usuarios.

[212] *Vid.* apéndice normativo.

[213] En su artículo 33 del Reglamento:
"*1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.*
2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.
3. La notificación contemplada en el apartado 1 deberá, como mínimo:
a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;
b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;
c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;
d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.
4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.
5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo."
Dicho artículo todavía no ha entrado en vigor, toda vez que la norma mencionada no será aplicable hasta el 25 de mayo de 2018. Entre otras cosas, para que las empresas afectadas tengan tiempo de adaptarse a sus previsiones.

5. OTROS ORGANISMOS VINCULADOS A LA PREVENCIÓN Y REPRESIÓN DE LA CIBERDELINCUENCIA

5.1 Organismos europeos:

En un entorno global como es internet, hábitat de la ciberdelincuencia, es necesario aportar respuestas globales, de forma que la labor que ejercen las instituciones que a continuación se relacionan es fundamental tanto en la coordinación entre los Estados como en los intercambios de información, aunque, en algunos casos la operatividad y coordinación efectiva no sea lo suficientemente rápida.

5.1.A) CENTRO EUROPEO DE CIBERDELINCUENCIA DE EUROPOL[214].

La Estrategia de seguridad interior de la Unión Europea en acción, adoptada el 22 de noviembre de 2010 por la Comisión[215] estableció la creación del Centro Europeo de Ciberdelincuencia de Europol (EC3) como una de las medidas destinadas a proteger a los ciudadanos de los ciberdelitos. Complementó a las propuestas legislativas, como la Directiva relativa a los ataques contra los sistemas de información y la Directiva relativa a la lucha contra la explotación sexual de la infancia en internet y la pornografía infantil. La misión en la lucha contra la ciberdelincuencia es desarticular las operaciones de las redes delictivas organizadas que cometen ciberdelitos. Apoya y coordina muchas de las operaciones e investigaciones llevadas a cabo por las autoridades de los Estados miembros.

5.1.B) EUROJUST[216].

Eurojust es la Unidad de Cooperación Judicial de la Unión Europea, creada en el año 2002 con el objetivo de estimular y mejorar la coordinación de las investigaciones y el ejercicio de las acciones penales, así como la cooperación entre las autoridades

[214] https://www.europol.europa.eu/ec3.
Se inauguró el 11 de enero de 2013 en la sede de Europol en La Haya, Países Bajos.

[215] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:ES:PDF.

[216] http://www.eurojust.europa.eu/Pages/languages/es.aspx.

competentes de los Estados miembros en relación a la delincuencia transfronteriza, entre la que se incluye la ciberdelincuencia como una de sus prioridades.

5.1.C) ENISA[217].

La Agencia Europea para la red y la seguridad de la información (ENISA)[218] es un centro de expertos para la ciberseguridad en Europa.

5.2 Organismos nacionales[219]:

5.2.A) CENTRO NACIONAL PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS (CNPIC)[220].

Órgano ministerial encargado del impulso, la coordinación y supervisión de todas las actividades que tiene encomendadas la Secretaría de Estado de Seguridad del Ministerio del Interior en relación con la protección de infraestructuras críticas en el territorio nacional.

Para el correcto ejercicio de sus funciones, el CNPIC mantiene estrechas relaciones tanto con otros departamentos de la Administración Pública, como con las empresas gestoras y propietarias de infraestructuras, tanto públicas como privadas.

5.2.B) INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE) y su CERT de Seguridad e Industria (CERTSI)[221].

Su principal objetivo es contribuir a mejorar el nivel de seguridad TIC (Tecnología de la Información y las Comunicaciones) para industria y ciudadanos. La prevención y concienciación, así como posteriormente dar soporte a las víctimas

[217] https://www.enisa.europa.eu

[218] ENISA, acrónimo del Ingles, the *European Union Agency for Network and Information Security*.

[219] Tal y como se refleja en la Estrategia de Ciberseguridad Nacional: (http://www.lamoncloa.gob.es/documents/20131332estrategiaciberseguridadx.pdf)

[220] http://www.cnpic.es/

[221] https://www.incibe.es/

ayudándoles para su desinfección[222]. Las principales líneas de trabajo son: promover servicios en el ámbito de la ciberseguridad que permitan el aprovechamiento de las TIC y eleven la confianza digital, la investigación y la coordinación[223].

5.2.C) MANDO CONJUNTO DE CIBERDEFENSA DE LAS FUERZAS ARMADAS (MCCD)[224].

Organismo de la estructura operativa, subordinado al Jefe de Estado Mayor de la Defensa (JEMAD), responsable de realizar el planeamiento y la ejecución de las acciones relativas a la ciberdefensa militar en las redes y sistemas de información y telecomunicaciones de las Fuerzas Armadas u otros que pudiera tener encomendados, así como contribuir a la respuesta adecuada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional.

[222] Adicionalmente, INCIBE trabaja en la detección proactiva de victimas de *botnets* para su desinfección.

[223] En concreto, INCIBE trabaja en la protección de la privacidad de los usuarios, fomenta el establecimiento de mecanismos para la prevención y reacción a incidentes de seguridad de la información, minimizando su impacto en el caso de que se produzcan, y promueve el avance de la cultura de la seguridad de la información a través de la concienciación, la sensibilización y la formación. Las empresas y organizaciones disponen de apoyo preventivo y reactivo en materia de seguridad en tecnologías de la información y la comunicación para aprovechar al máximo las posibilidades de las TIC de forma segura y confiable.
Los Focos de atención de INCIBE son:

- Empresas y profesionales que hacen uso de las TIC: Con especial atención, INCIBE destina esfuerzos para la protección de los sectores estratégicos, imprescindibles para la economía y la sociedad, así como a las instituciones afiliadas a RedIRIS.
- Expertos en ciberseguridad: a través del equipo especializado en ciberseguridad, INCIBE ofrece servicios de información y respuesta a colectivos y profesionales expertos para mejorar los niveles de ciberseguridad en España.
- Ciudadanos: la Oficina de Seguridad del Internauta (OSI) http://www.osi.es es el servicio gratuito que proporciona información y soporte al usuario final para evitar y resolver los problemas de seguridad que le pueden surgir al navegar por internet, sobre todo en sus primeros pasos en las nuevas tecnologías.

INCIBE cuenta con una importante capacidad para abordar proyectos complejos de diversa naturaleza y con una fuerte componente innovadora. La dinámica de sus operaciones está asimismo orientada a la investigación, lo que permite que cuente con capacidad para generar inteligencia en ciberseguridad como motor para abordar su aplicación en nuevas tecnologías y mecanismos que reviertan también en la mejora de los servicios.
INCIBE participa en redes de colaboración que facilitan la inmediatez, globalidad y efectividad a la hora de desplegar una actuación en el ámbito de la ciberseguridad, contando siempre con una perspectiva basada en la experiencia y en el intercambio de información. Por ello, la coordinación y colaboración con otras entidades, tanto públicas como privadas, nacionales e internacionales, de todo el ámbito de la ciberseguridad es un factor imprescindible para la actividad de INCIBE.

[224] http://www.emad.mde.es/CIBERDEFENSA/

5.2.D) EL CENTRO CRIPTOLÓGICO NACIONAL-CERT (CCN-CERT), es la capacidad de respuesta a incidentes de seguridad de la información del Centro Criptológico Nacional (CCN)[225].

Es competencia del CCN-CERT la gestión de ciberincidentes que afecten a sistemas clasificados de las Administraciones Públicas (General, Autonómica y Local), de empresas y organizaciones de interés estratégico para el país. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

En lo que se refiere a la represión de la ciberdelincuencia está fuera de su ámbito. Desde el CCN-CNI el foco se ciñe al ciberespionaje, aunque se llevan a cabo acciones de concienciación ante las ciberamenazas en sentido amplio en numerosos foros públicos y privados, y es también su competencia formar al personal funcionario de las Administraciones Públicas en diferentes aspectos de la ciberseguridad. En este sentido, aunque la preocupación principal de este organismo sigue siendo el ciberespionaje, es cierto que muchas de las TTP (técnicas, tácticas y procedimientos) son comunes entre los diferentes actores de la amenaza y, por tanto, también las recomendaciones de seguridad que se ofrecen.

Asimismo, el CCN-CERT dispone de sistemas de detección temprana de ataques desplegados en las Administraciones Públicas y empresas de interés estratégico, por lo que se notifican ataques informáticos relacionados con el mundo de la ciberdelincuencia (*Ej: troyanos bancarios, ransomware, botnets, etc.).*

[225] www.ccn.cni.es Este servicio se creó en el año 2006 como el CERT Gubernamental Nacional español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el Real Decreto 421/2004 regulador del Centro Criptológico Nacional y en el Real Decreto 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS).

5.3 Entidades del tercer sector (asociaciones, ONGs Y fundaciones) que son actores relevantes en la labor de prevención y represión de la ciberdelincuencia:

En concreto, en lo relativo al colectivo de menores, debido a su cercanía con la ciudadanía, promueven la sensibilización y sirven de punto de apoyo para canalizar las denuncias a las Fuerzas y Cuerpos de Seguridad del Estado. Estas entidades tienen su representación en el grupo de trabajo público-privado que gestiona *Red.es,* y en el que están involucrados los principales actores vinculados a la protección del menor en internet (Administración General del Estado, industria, tercer sector)[226].

[226] Algunas de las entidades del tercer sector más relevantes:

- *Pantallas Amigas*. Organización sin ánimo de lucro, que tiene como misión la promoción del uso seguro y saludable de las nuevas tecnologías y el fomento de la ciudadanía digital responsable en la infancia y la adolescencia. http://www.pantallasamigas.net. 22/4/2016 a las 14.25

- *Fundación Alia2*[226]. Entidad sin ánimo de lucro que trabaja para proteger los derechos de los menores en internet, fomentando un uso seguro y responsable de la red. http://alia2.org/index.php/es/inicio. 22/4/2016 a las 14.20

- *Padres 2.0.*[226]. Organización sin ánimo de lucro en España que ofrece un tratamiento integral frente a los riesgos derivados de las nuevas tecnologías (TIC): prevención, sensibilización, formación, mediación y asistencia psicológica y jurídica. http://padres20.org. 22/4/2016 a las 14.10

- *Fundación Anar*[226]. Organización sin ánimo de lucro, que se dedica en el marco de la Convención de los Derechos del Niño de Naciones Unidas, a la promoción y defensa de los derechos de los niños y adolescentes en situación de riesgo y desamparo, mediante el desarrollo de proyectos. http://www.anar.org. 22/4/2016 a las 14.15

Por último, la Universidad de Alcalá de Henares (UAH) a través de la "*Cátedra Amaranto, seguridad digital e internet de futuro"* impulsa y forma parte de manera principal y proactiva del Foro de colaboración Público/Privada en Ciberseguridad centrado en el poder Legislativo / Judicial. El Foro surge con la idea de fomentar los mecanismos necesarios para realizar acciones que propicien la colaboración público-privada en materia de ciberseguridad, así como fomentar un sistema de gestión del conocimiento relacionado con la misma, dando soporte a todas las partes interesadas, desde los ámbitos tecnológicos, legales y físicos hacia el poder jurídico/legal. http://catedraamaranto.cc.uah.es 22/04/2016 a las 14.30. Forman parte del Foro, a título personal, nunca representando a sus organizaciones: Letrados de las Cortes Generales (Senado y Congreso), personal de Fiscalía de Sala de Criminalidad Informática, personal del Cuerpo Nacional de Policía , de la Guardia Civil, del Mando Conjunto de Ciberdefensa, del Centro Criptológico Nacional. Personas vinculadas al mundo universitario (UAH y UAM). Personas del sector privado (Telefónica, CaixaBank, Bankia, BBVA, E&Y, Eulen Seguridad, Ferrovial, Iberdrola, Repsol, etc...). El programa denominado "Quijote" herramienta diseñada para la localización de los usuarios que comparten material pedófilo fue creado por alumnos de la Cátedra Amaranto de Seguridad Digital e Internet del Futuro.

CAPÍTULO SEXTO

DERECHOS Y LIBERTADES QUE RESULTAN AFECTADOS.

La investigación de los ciberdelitos puede afectar a varios derechos fundamentales dependiendo de la diligencia de investigación interesada. Así, por ejemplo, el acceso a la información contenida en los dispositivos electrónicos por parte del sistema penal puede afectar a la intimidad personal (art. 18.1 CE), al secreto de las comunicaciones (art. 18.3 CE) y a la protección de datos personales (art. 18.4 CE), o a lo que algún autor ha denominado *el derecho a la identidad virtual*[227]. También puede verse afectado el derecho a la inviolabilidad domiciliaria (art. 18.2 CE) en aquellos supuestos en los que el dispositivo electrónico se halle en el curso de una entrada y registro en domicilio[228]. Es por ello, que la propia LECrim, en la redacción dada por la *Ley Orgánica 13/2015, de 5 de octubre,* regula diversas medidas de investigación en el Título VIII del Libro II, precisamente bajo la rúbrica "*De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución"*.

El propio preámbulo de la ley justifica la reforma de la LECrim porque resulta preciso afrontar de inmediato la regulación de las medidas de investigación tecnológica en el ámbito de los derechos a la intimidad, al secreto de las comunicaciones y a la protección de datos personales garantizados por la Constitución.

---

[227] ZARAGOZA TEJADA, J. I., La reforma operada por Ley 13/2015. El Agente Encubierto Informático. Ponencia presentada en el curso de Formación de Fiscales "Uso de las nuevas tecnologías y nuevas formas de delincuencia" que se celebró en el Centro de Estudios Jurídicos los días 27 al 28 de octubre de 2016 VALVERDE MEGÍAS, R., Intervención de comunicaciones telemáticas y registro remoto. Ponencia presentada en el curso de Formación de Fiscales "Uso de las nuevas tecnologías y nuevas formas de delincuencia" que se celebró en el Centro de Estudios Jurídicos los días 27 al 28 de octubre de 2016 CONDE-PUMPIDO TOURÓN, C. "La reforma procesal. Registro de sistemas informáticos, ampliación del registro a otros sistemas. El registro remoto de dispositivos informáticos (arts 588 sexies y 588 septies LECrim). Ponencia presentada en las Jornadas de especialistas de criminalidad informática. 2016. www. Cej-mjusticia.es. .

[228] DELGADO MARTIN, J, "Derechos fundamentales afectados en el acceso al contenido de dispositivos electrónicos para la investigación de delitos". Diario La Ley nº 8202, Sección Doctrina, 29 Nov. 2013. Versión electrónica, págs. 1-20.

En este capítulo se analiza la naturaleza de cada uno de los derechos fundamentales afectados por las diferentes diligencias de investigación, y en qué medida han de practicarse estas diligencias para que quede debidamente garantizada la protección de estos derechos fundamentales.

Como norma general cualquier diligencia de investigación criminal que afecte a derechos fundamentales, exige, salvo supuestos excepcionales, autorización judicial dictada en el curso de un procedimiento judicial de investigación. A su vez nuestros Tribunales han ido fijando las condiciones en que ha de hacerse esa intervención para garantizar debidamente la protección de los derechos fundamentales, creando un cuerpo de doctrina aplicable a los supuestos de injerencia, sin consentimiento del interesado, en el ámbito de privacidad[229], que concretó nítidamente la Sentencia del Tribunal Constitucional 173/2011, de 7 de noviembre, en[230]:

a) La existencia de un fin constitucionalmente legítimo.

b) Previsión legal de la medida limitativa del derecho.

c) Proporcionalidad de la medida definida a través del juicio de idoneidad, necesidad y proporcionalidad en sentido estricto.

d) Autorización judicial motivada salvo en los supuestos de intervención policial por razones de urgencia y necesidad y siempre que, en este último caso, no exista reserva constitucional a favor de la autoridad judicial.

En líneas generales, cuando se trata de investigación de ciberdelitos y uso de nuevas tecnologías, los derechos fundamentales más afectados son el derecho a la intimidad y el derecho al secreto de las comunicaciones, a los que hay que añadir el derecho a la protección de datos de carácter personal o el derecho al propio entorno virtual como una categoría que engloba a las anteriores:

[229] *Vid*. GONZÁLEZ-CUELLAR SERRANO, N. "Proporcionalidad y derechos fundamentales en el proceso penal", Ed. Colex, Madrid, 1990.

[230] Anteriormente recogida en SSTC 207/1996 de 16 de diciembre; 70/2001 de 3 de abril; 89/2006 de 27 de marzo. Y posteriormente en STC 142/2012, de 2 de julio y STS 786/2015, de 4 de diciembre.

- El derecho a la intimidad (art. 18.1) y el derecho a la protección de datos (art. 18.4 CE) son de naturaleza material, de origen natural y modulable por el ciudadano que puede decidir sobre los límites de protección. Está regulado, además de por la L.O. 1/1982, de 5 de mayo (en cuanto a la intimidad), por la Ley Orgánica 15/1999, de 13 de Diciembre, de protección de datos de carácter personal, que permite el acceso a los mismos por la policía.

- El derecho al secreto de las comunicaciones (art. 18.3 CE) es de naturaleza formal, de configuración legal y protegible sin modulaciones. Se encuentra regulado por la Ley 25/2007, de 18 de Octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

Nuestras normas procesales han carecido durante muchos años de una regulación precisa en materia de investigaciones restrictivas de estos derechos fundamentales, lo que ha venido a motivar, incluso, varias resoluciones del Tribunal Europeo de Derechos Humanos (TEDH) recordando a nuestro Estado la necesidad de la misma. Esa laguna en nuestro derecho positivo, no obstante, ha sido cubierta durante todos estos años por la jurisprudencia que, a través de sus resoluciones, ha llegado a establecer en nuestro ordenamiento jurídico un cuerpo de doctrina que sintetiza la emanada del propio TEDH, supliendo así esa falta de regulación legal.

La introducción en la LECrim, por medio de la Ley Orgánica 13/2015, de 5 de octubre, de la regulación de medidas de investigación tecnológica, si bien ha supuesto el fin de esa orfandad legal, en ningún caso ha significado la inaplicación de la profusa doctrina jurisprudencial, ya que, al tomar la nueva regulación como fundamento la misma doctrina del TEDH, se ha mantenido la misma línea desarrollada por nuestra jurisprudencia, con lo que, la interpretación que nuestros Tribunales venían haciendo de la doctrina del TEDH, resulta plenamente vigente para interpretar también ahora la nueva regulación legal.

Veamos cada uno de los derechos fundamentales que resultan afectados a la luz de la doctrina del TEDH en su interpretación del Convenio Europeo de Derechos

Humanos (CEDH)[231], de la Constitución Española, de nuestros Tribunales (Constitucional y Supremo), y por supuesto de nuestra doctrina científica.

1. EL DERECHO A LA INTIMIDAD.

El art. 8.1 del CEDH reconoce el derecho al respeto de la vida privada y familiar. En la Constitución Española, el derecho a la intimidad personal y familiar se regula en el artículo 18.1 junto al derecho al honor y a la propia imagen. Son tres derechos autónomos y sustantivos, aunque estrechamente vinculados entre sí, en tanto que derechos de la personalidad, derivados de la dignidad humana y dirigidos a la protección del patrimonio moral de las personas[232], por lo que estos tres derechos podrán verse afectados, de manera independiente, pero también, con frecuencia, de forma conjunta, dada su evidente proximidad[233].

La intimidad, es un bien jurídico que la Constitución Española ha elevado a la categoría de derecho fundamental, vinculado con el libre desenvolvimiento de la

[231] Circular 1/2013 sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas. *Debe recordarse que las resoluciones del TEDH tienen valor vinculante. Conforme al art. 46 CEDH, los Estados parte se comprometen a acatar las sentencias definitivas dictadas por el Tribunal Europeo de Derechos Humanos en los litigios en que sean parte. No solamente tienen valor jurídico las resoluciones de condena en relación con el Estado condenado. Igualmente debe reconocerse un rol capital a la doctrina del TEDH, de valor incuestionable. En este sentido ha declarado el TC que "la Jurisprudencia del TEDH…de conformidad con lo dispuesto en el artículo 10.2 de nuestra Constitución, ha de servir de criterio interpretativo en la aplicación de los preceptos constitucionales tuteladores de los derechos fundamentales y que es de "aplicación inmediata en nuestro ordenamiento jurídico"* (STC nº 303/1993, de 25 de octubre [FJ 8º].

[232] STC 14/2003, de 28 de enero [FJ 4].

[233] El desarrollo de la protección de estos derechos lo efectúa, principalmente, la LO 1/1982, de 5 de mayo, de protección civil del derecho al honor, la intimidad y la propia imagen, en la que se intentan deslindar los supuestos de intromisión ilegítima (art. 7), de aquellos que no puedan reputarse como tales, por mediar consentimiento o por recoger imágenes públicas (art. 8). Junto a esta Ley hay que mencionar igualmente la protección penal a través de los delitos de injurias y calumnias (arts 205-210; 491, 496, 404-5 CP), y la que ofrece la LO 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, desarrollada por el Real Decreto 596/1999, de 16 de abril, donde se establecen, por lo que a la garantía de la intimidad se refiere, desde la información sobre la existencia de videocámaras a la destrucción de las grabaciones, salvo las que contengan imágenes relacionadas con infracciones penales o administrativas graves, con la correspondiente obligación de reserva por parte de los que tengan acceso a las imágenes (art. 8 y 9 LO 4/1997).

personalidad y presupuesto del ejercicio potencial y pleno de otros derechos y libertades constitucionales[234].

El art. 18 CE acoge un contenido amplio de la intimidad personal y familiar que varía en función de las ideas y convicciones más generalizadas en la sociedad en cada momento histórico[235]. La STC 115/2000, de 5 de mayo afirma que "*el derecho fundamental a la intimidad reconocido por el art. 18.1 CE tiene por objeto garantizar al individuo un ámbito reservado de su vida, vinculado con el respeto a su dignidad como persona (art. 10.1 CE), frente a la acción y el conocimiento de los demás, sean éstos poderes públicos o simples particulares"*. De esta manera, la protección de ese ámbito reservado confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima y la prohibición de hacer uso de lo así conocido (STC 115/2013, de 9 de mayo [FJ 5].

En los últimos años ha cobrado una gran importancia la necesidad de protección de la intimidad frente a los nuevos medios de investigación generados tras el desarrollo de las tecnologías, como aquellos que implican la utilización de la videovigilancia[236] o el uso de los dispositivos electrónico de captación y grabación de comunicaciones orales o de captación de la imagen, de seguimiento y de localización[237].

En general, todas aquellas diligencias de investigación en las que pueda resultar afectado el derecho a la intimidad (piénsese por ejemplo, en el registro de un ordenador personal) le son aplicables las garantías que legitiman la injerencia en ese derecho

---

[234] *Vid.* MORALES PRATS, F. "Los delitos contra la intimidad en el Código Penal de 1995: reflexiones político-criminales", en Cuadernos de Derecho Judicial, volumen dedicado a "Estudios sobre el Código Penal de 1995 (parte especial)". Ed. CGPJ y la Escuela Judicial, Madrid, 1996, págs. 243 y ss.; y LÓPEZ ORTEGA, J. J. "La intimidad como bien jurídico protegido," en Cuadernos de Derecho Judicial, volumen dedicado a "Estudios sobre el Código Penal de 1995 (parte especial)" Ed. CGPJ y Escuela Judicial, Madrid, 1996, págs. 287 y ss.

[235] *Vid* la STC 171/1990, de 12 de noviembre [FJ 5].

[236] Desarrollada por la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.

[237] Regulado en el Título VIII del Libro II de la Ley de Enjuiciamiento Criminal "*De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución"*, tras la modificación introducida por *Ley Orgánica 13/2015, de 5 de octubre.*

fundamental durante la investigación del delito[238], cuyo incumplimiento determinará la ilicitud de la prueba y su nulidad[239].

1.1 Requisitos para la injerencia.

El TEDH[240], interpretando el art. 8 CEDH estima que la injerencia del Estado en la vida privada puede resultar justificada siempre que concurran tres requisitos:

- Que la finalidad sea legítima (legitimidad del fin).

- Que la injerencia esté prevista por la ley (legalidad).

- Y, por último, que sea necesaria en una sociedad democrática para la consecución de ese fin (necesidad)[241].

Esta doctrina ha sido recogida y desarrollada por la jurisprudencia constitucional española (STC 115/2013, de 9 de mayo [FJ 5][242]. Estos presupuestos resultan plenamente aplicables a la injerencia en el derecho a la intimidad por aquellas diligencias de investigación que afectan al mismo, como puede ser el registro de un sistema informático.

La reforma de la LECrim de octubre de 2015 considera oportuna la proclamación normativa de los principios que el Tribunal Constitucional había definido como determinantes de la validez del acto de injerencia:

---

[238] ASENCIO MELLADO, J. M. "Prueba ilícita: declaración y efectos", en Revista General de Derecho, nº 26, año 2012, pág. 15.

[239] *Vid.* MARCOS GONZÁLEZ, M. "Doctrina constitucional sobre la prueba ilícita: discrepancias interpretativas". La Ley Penal nº 88, Sección Estudios, Dic. 2011.

[240] STEDH (Sección 4ª) 3 de abril de 2007, caso *Copland* contra Reino Unido. STEDH (Gran Sala) 4 de mayo de 2000, caso *Rotaru* contra Rumanía.

[241] *Vid.* MORENILLA RODRÍGUEZ, J. M. "El derecho al respeto de la esfera privada en la jurisprudencia del Tribunal Europeo de Derechos Humanos", en Cuadernos de Derecho Judicial, volumen dedicado a "La Jurisprudencia del Tribunal Europeo de Derechos Humanos". Ed. CGPJ, Madrid, 1993, págs. 322 y ss.

[242] STC 70/2001 de 3 de abril [FJ 10] y la STC 173/2011, de 7 de noviembre [FJ 2º] y la jurisprudencia allí citada.

- En primer lugar, la existencia de un fin constitucionalmente legítimo, es decir el interés público propio de la prevención e investigación del delito y, más en concreto, la determinación de hechos relevantes para el proceso penal mediante la prueba informática.

- En relación con el segundo presupuesto, el principio de legalidad, las dudas que surgían en relación al mismo por cuanto no existía en la LECrim una regulación específica acerca de las diligencias de investigación tecnológica como pudieran ser el registro y ocupación del contenido de los dispositivos electrónicos[243], quedaron disipadas tras la reforma de la LECrim por la *Ley Orgánica 13/2015,* que integra el vacío legal a través de la introducción de diferentes normas relativas a diligencias de investigación tales como: la interceptación de las comunicaciones telefónicas y telemáticas, captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos.

- Por último, las medidas de investigación tecnológica necesitan autorización judicial previa, que lleve a cabo una ponderación de los bienes en conflicto en el caso concreto, deben además satisfacer los principios de idoneidad, excepcionalidad, necesidad y proporcionalidad, cuya concurrencia ha de encontrarse suficientemente justificada en la resolución judicial habilitadora, donde el juez determinará la naturaleza y extensión de la medida en relación con la investigación concreta y con los resultados esperados; salvo los supuestos de consentimiento del afectado o de urgente intervención policial en aquellos casos donde no exista reserva a favor de la autoridad judicial.

[243] Se justificaba su adopción en varios preceptos legales habilitantes como el art. 546 LECrim que permitía el registro de *efectos o instrumentos del delito, o libros, papeles u otros objetos que puedan servir para su descubrimiento o comprobación*, aunque lo hace en el seno de la regulación de la entrada y registro en lugar cerrado; así como incluso en los arts. 326.1º y 574 LECrim., que permitían el primero de ellos al juez la recogida de las pruebas materiales de la perpetración del delito y su inspección ocular.

Veamos, de forma más pormenorizada, estos presupuestos:

1.1.A) La Autorización Judicial.

Se ha estimado oportuna la proclamación normativa de los principios que el Tribunal Constitucional considera determinantes de la validez del acto de injerencia: especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida.

Así, toda autorización judicial ha de ser dictada con plena sujeción a dichos principios[244].

- El principio de especialidad exige que una medida esté relacionada con la investigación de un delito concreto, lo que significa que no podrán autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin una base objetiva. Un acto instructorio que limite un derecho fundamental no puede estar dirigido exclusivamente a obtener meros indicios o sospechas de criminalidad, sino debe tener como finalidad la preconstitución de la prueba de los hechos que integran el objeto del proceso penal (STC 207/1996, de 16 de

[244] *Artículo 588 bis a. Principios rectores.*
1. Durante la instrucción de las causas se podrá acordar alguna de las medidas de investigación reguladas en el presente capítulo siempre que medie autorización judicial dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida.
2. El principio de especialidad exige que una medida esté relacionada con la investigación de un delito concreto. No podrán autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva.
3. El principio de idoneidad servirá para definir el ámbito objetivo y subjetivo y la duración de la medida en virtud de su utilidad.
4. En aplicación de los principios de excepcionalidad y necesidad 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.
5. 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.

diciembre)[245]. Se prohíben pues las medidas de investigación tecnológica de naturaleza prospectiva, de acuerdo con el concepto que informa la doctrina emanada del máximo intérprete de la Constitución (por todas la sentencia 253/2006, de 11 de septiembre[246]).

- El principio de idoneidad se refiere al ámbito objetivo y subjetivo y a la duración de la medida en virtud de su utilidad. Debe existir una relación de adecuación entre el medio de investigación y el fin perseguido. De esta forma, aquél debe servir objetivamente para la finalidad constitucionalmente legítima: conseguir datos útiles para investigar las circunstancias del delito[247].

- En aplicación de los principios de excepcionalidad y necesidad solo podrá acordarse la medida cuando no estén a disposición de la investigación otras medidas menos gravosas para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho, o 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. En definitiva, nos encontramos ante una cláusula de subsidiariedad, de tal manera que el medio seleccionado para alcanzar el fin no pueda ser suplido por otro igualmente eficaz, pero que no restrinja el derecho fundamental o lo haga de una manera menos gravosa[248].

- Por el principio de proporcionalidad en sentido estricto, las medidas de investigación 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

[245] La STC 207/1996, de 16 de diciembre se refiere a un supuesto relativo a la extracción de cabello de distintas partes del cuerpo para su posterior análisis que tenía por objeto conocer si la persona (agente de la Guardia Civil al que se imputa un delito de cohecho) era consumidora de droga.

[246] STC 219/2009, de 21 de diciembre.

[247] Como afirma el de La STC 207/1996, de 16 de diciembre [FJ 4º] "*la medida debe ser idónea (apta, adecuada) para alcanzar el fin constitucionalmente legítimo perseguido con ella (art. 8 CEDH), esto es, que sirva objetivamente para determinar los hechos que constituyen el objeto del proceso penal".*

[248] *Vid.* PEDRAZ PENALVA, E y ORTEGA BENITO, V., "El principio de proporcionalidad y su configuración en la jurisprudencia del Tribunal Constitucional y literatura especializada alemanas", en Poder Judicial, núm. 17, 1990, pág. 17.

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[249].

- La resolución judicial motivada debe plasmar el juicio de ponderación entre el derecho fundamental afectado y el interés constitucionalmente protegido y perseguido, del cual se evidencie la necesidad de la adopción de la medida[250]. La resolución se adoptará oído el Ministerio Fiscal (art. 588 bis c de la LECrim) y concretando los siguientes extremos[251]:

a) El hecho punible objeto de investigación y su calificación jurídica, con expresión de los indicios racionales en los que funde la medida.

b) La identidad de los investigados y de cualquier otro afectado por la medida, de ser conocido.

---

[249] Como afirma GONZÁLEZ-CUELLAR SERRANO, N. "Proporcionalidad y derechos fundamentales (…) ob. cit. pág. 225, este principio tiene como finalidad la determinación, mediante la utilización de las técnicas del contrapeso de los bienes o valores y la ponderación de intereses según las circunstancias del caso concreto, si el sacrificio de los intereses individuales que comporta la injerencia guarda una relación razonable o proporcionada con la importancia del interés estatal que se trata de salvaguardar. Para que el acceso al dispositivo electrónico resulte proporcional en el caso concreto, deben tenerse en cuenta varios criterios:
a) Criterio de la expectativa de las consecuencias jurídicas del delito, es decir, deberá tenerse en cuenta la gravedad de la pena señalada al delito que se está investigando.
b) Criterio de la importancia de la causa que, entre otras circunstancias, viene determinada por la naturaleza del bien jurídico lesionado, las concretas formas de manifestación del hecho (la habitualidad en la comisión delictiva, la peligrosidad social de los efectos del hecho, etc.) y las circunstancias relevantes en la persona del imputado (la tendencia a cometer hechos de la misma naturaleza o la especial intensidad del comportamiento delictivo) .
c) Criterio del grado de imputación. El Estado podrá restringir un derecho fundamental sólo en aquellos supuestos en los que exista un grado suficiente de imputación de un delito, es decir, cuando existan razones objetivas que permitan afirmar la probabilidad de que se haya cometido un delito. En otro caso, se estaría otorgando a los órganos estatales una patente de corso para inmiscuirse en la vida privada de los ciudadanos inadmisible en un Estado de Derecho. Es exigible la concurrencia de indicios, y no meras sospechas, de la existencia del delito objeto de la investigación; evitando de esta manera investigaciones prospectivas.

[250] STC 48/2009 de 15 de junio.

[251] Aunque la jurisprudencia admitía la llamada motivación por remisión siempre que, al ser integrada con la solicitud policial o informe del fiscal al que se remita, se contengan todos los elementos necesarios para llevar a cabo el juicio de proporcionalidad (STC 25/2011, 14 de marzo). Con la nueva reforma de la LECrim será necesario que el auto recoja toda la argumentación que fundamente la autorización, pues precisamente con el fin de evitar que las resoluciones judiciales adolezcan de un laconismo argumental susceptible de vulnerar el deber constitucional de motivación, se orienta la minuciosa regulación del contenido de esa solicitud, así como de la resolución judicial que, en su caso, habilite la medida de injerencia.

c) La extensión de la medida de injerencia, especificando su alcance así como la motivación relativa al cumplimiento de los principios rectores establecidos en el artículo 588 bis a.

d) La unidad investigadora de Policía Judicial que se hará cargo de la intervención.

e) La duración de la medida.

f) La forma y la periodicidad con la que el solicitante informará al juez sobre los resultados de la medida.

g) La finalidad perseguida con la medida.

h) El sujeto obligado que llevará a cabo la medida, en caso de conocerse, con expresa mención del deber de colaboración y de guardar secreto, cuando proceda, bajo apercibimiento de incurrir en un delito de desobediencia.

1.1.B) Consentimiento del afectado.

Con carácter general, el consentimiento del afectado legitima la injerencia en el derecho a la intimidad porque corresponde a cada persona acotar el ámbito de intimidad personal y familiar que reserva al conocimiento ajeno (STC 83/2002, de 22 de abril [FJ 5º]; STC 196/2006, de 3 de julio [FJ 5º] y STC 173/2011, de 7 de noviembre), aunque dicho consentimiento puede ser revocado en cualquier momento (STC 159/2009, de 29 de junio [FJ 3º].

En este sentido, la STC 206/2007, de 24 de septiembre, entiende que "*se vulnerará el derecho a la intimidad personal cuando la penetración en el ámbito propio y reservado del sujeto no sea acorde con la Ley, no sea eficazmente consentida o, aun autorizada, subvierta los términos y el alcance para el que se otorgó el consentimiento, quebrando la conexión entre la información personal que se recaba y el objetivo*

tolerado para el que fue recogida"[252]. Esta doctrina ha de resultar de aplicación a cualquier injerencia en el derecho a la intimidad, también cuando se realiza mediante el empleo de las medidas de investigación tecnológica. Así como establece la STC 173/2011, de 7 de noviembre, cualquier injerencia en el contenido de un ordenador personal, ya sea por vía de acceso remoto a través de medios técnicos, ya sea por vía manual, deberá venir legitimada en principio por el consentimiento de su titular, o bien por la concurrencia de los presupuestos habilitantes antes citados [FJ 4º].

El consentimiento no necesita ser escrito, pudiendo ser verbal (STC 173/2011, de 7 de noviembre [FJ 5º]. Asimismo la jurisprudencia constitucional admite también la eficacia del consentimiento tácito, que ha de derivarse de actos concluyentes. Por ello resulta necesario exigir que la persona afectada sea informada adecuadamente sobre la diligencia para la cual presta consentimiento[253].

Téngase en cuenta que se vulnera el derecho a la intimidad personal cuando la penetración en el ámbito propio y reservado del sujeto aún autorizada, subvierta los términos y el alcance para el que se otorgó el consentimiento, quebrando la conexión entre la información personal que se recaba y el objetivo tolerado para el que fue recogida[254].

---

[252] En la misma línea, la STS 277/2007 de 13 de abril, referida a un cacheo en un proceso por delito contra la salud pública, recuerda que *el consentimiento, además, puede actuar como fuente legitimadora del acto de injerencia. Dicho en palabras de la misma jurisprudencia constitucional, debe recordarse que el derecho a la intimidad no es un derecho absoluto, sino que puede ceder ante intereses constitucionalmente relevantes siempre que (...) exista un consentimiento eficaz que lo autorice, pues corresponde a cada persona acotar el ámbito de intimidad personal y familiar que reserva al conocimiento ajeno.*

[253] En este sentido, la STC 206/2007, de 24 de septiembre, afirma que no existe constancia alguna de que fuera informado expresamente de la prueba que se pretendía practicar (análisis de sangre) y de la finalidad de la misma (determinar la tasa de alcohol en sangre o la presencia de otras sustancias estupefacientes), una prueba que resultaba ajena a toda finalidad terapéutica y que, por ello, no resultaba previsible para quien es sometido a pruebas médicas por el personal facultativo de un centro hospitalario en el que se encuentra ingresado tras sufrir un accidente de tráfico. Siendo así, ha de descartarse la presencia de un consentimiento informado eficaz del afectado que legitime la medida, aun partiendo de la premisa fáctica de que existiera consentimiento en la extracción de sangre (por todas, STC 196/2004, de 15 de noviembre [FJ 9º].

[254] (STC 196/2004, de 15 de noviembre [FJ 2º]; STC 206/2007, de 24 de septiembre [FJ 5º]; STC 70/2009, de 23 de marzo [FJ 2º]; STC 173/2011, de 7 de noviembre [FJ 2º].

En el caso abordado en la STC 173/2011, de 7 de noviembre[255], el recurrente acudió al establecimiento de informática que regentaba el denunciante y le hizo entrega de su ordenador portátil con el encargo de cambiar una grabadora que no funcionaba. El encargado del establecimiento procedió a la reparación, y para comprobar el correcto funcionamiento de las piezas eligió al azar varios archivos para su grabación y posterior reproducción. Para ello accedió a la carpeta "mis documentos/mis imágenes" del ordenador, encontrando diversos archivos fotográficos de contenido pedófilo que motivaron la interposición de la denuncia. El TC descartó en este caso la vulneración del derecho a la intimidad al estimar un consentimiento tácito del afectado, pues aunque no autorizó de forma expresa al informático el acceso al contenido de sus archivos o ficheros donde se encontraban las fotografías y videos de contenido pedófilo, consideró que su conducta no se extralimitó del mandato conferido, añadiendo el Tribunal que "*avala esta conclusión la circunstancia de que este encargado limitara su actuación a la carpeta "mis documentos" del usuario, mínimo necesario para realizar la referida prueba de grabación, sin pretender adentrarse en otras carpetas respecto de las que, por hallarse más ocultas o por expresarlo así el título asignado a las mismas, pudiera presumirse un mayor revestimiento de protección y reserva. Seguidamente, una vez producido el hallazgo, este se limitó a cumplir con la obligación que le viene legalmente impuesta a todo ciudadano consistente en denunciar ante las autoridades competentes la posible perpetración de un delito público del que ha tenido conocimiento (arts. 259 y ss. LECrim.)"* [FJ 5º].

Sin embargo, dicho argumento no está exento de crítica porque en realidad no existió un consentimiento del titular que abarcara el examen de los archivos por parte del informático, ni expreso ni tácito; ni tampoco éste le informó previamente de la necesidad de examinar archivos para comprobar el funcionamiento adecuado de la grabadora instalada[256]. Un razonamiento más que discutible cuando está en juego el derecho a la intimidad.

[255] Doctrina Constitucional posteriormente recogida en la STS 786/2015, de 4 de diciembre.

[256] CONTRERAS CEREZO P. "Comentario a la STC 173/2011". Diario La Ley nº 7819, Sección La Sentencia del día del TC, marzo 2012 afirma que una reparación no puede justificar la visualización de archivos gráficos del ordenador cuando existen alternativas que permiten verificar lo adecuado de la reparación, bastaría con utilizar un disquete o CD con imágenes para visionarlos con la grabadora que se reparó. Mas bien parece exigible a los encargados de establecimientos de reparaciones de este tipo que adviertan a los clientes de la necesidad de tener que visionar archivos gráficos del ordenador para que

1.1.C) Intervención policial por razones de urgencia y necesidad.

La Constitución contiene una reserva absoluta de resolución judicial en determinadas medidas restrictivas de derechos fundamentales que pueden ser adoptadas en el curso del proceso penal, como las entradas y registros en domicilio (art. 18.2 CE) o la intervención de las comunicaciones (art. 18.3 CE). En cambio, no existe expresamente dicha reserva en relación con las actuaciones que afecten al derecho a la intimidad (art. 18.1 CE). No obstante, la jurisprudencia ha admitido de forma excepcional que en determinados casos y con la suficiente y precisa habilitación legal sea posible que la policía judicial realice determinadas prácticas que constituyan una injerencia leve en la intimidad de las personas, siempre que respeten las exigencias dimanantes del principio de proporcionalidad, y existan razones de urgencia y necesidad que motiven la intervención policial inmediata[257].

Siguiendo la doctrina del TC, cabe afirmar que los requisitos que proporcionan una justificación constitucional objetiva y razonable a la injerencia policial en el derecho a la intimidad[258], son además de los ya examinados de fin constitucionalmente legítimo y habilitación legal, la urgencia y la necesidad en la intervención.

Al respecto, la doctrina constitucional sostiene "*que la valoración de la urgencia y necesidad de la intervención policial ha de realizarse ex ante, y es susceptible de control judicial ex post, al igual que el respeto del principio de proporcionalidad; la*

estos puedan expresar su consentimiento sobre dicha circunstancia. "*El acceso a la información acumulada en un ordenador pertenece al ámbito de la intimidad. Su acceso, por la policía judicial no consentido por su propietario o sin autorización judicial personal, sólo será constitucionalmente legítimo si existen razones de necesidad y urgencia y respeta los principios de proporcionalidad y razonabilidad*".

[257] Como afirma la STS 691/2009, de 5 de junio, "*de la Sentencia del Tribunal Constitucional 281/2006 de 9 de octubre se puede concluir que no existe en la Constitución reserva absoluta de previa resolución judicial respecto a derecho a la intimidad personal y excepcionalmente se admite la legitimidad constitucional de que en determinados casos, y con precisa habilitación legal, pueda la Policía Judicial realizar determinadas prácticas que constituyen una leve injerencia en la intimidad de las personas siempre que se respeten las sugerencias derivadas del principio de proporcionalidad"*.
La STC 115/2013, de 9 de mayo, permite que en algunos casos y con la suficiente y precisa habilitación legal, la policía realice determinadas prácticas que constituyan una injerencia leve en la intimidad de las personas sin previa autorización judicial (y sin consentimiento del afectado), siempre que se hayan respetado las exigencias dimanantes del principio de proporcionalidad (por todas, SSTC 70/2002, de 3 de abril[FJ 10]; 123/2002, de 20 de mayo [FJ 4º]; 56/2003, de 24 de marzo [FJ 2.º]; 281/2006, de 9 de octubre [FJ 4º]; y 142/2012, de 2 de Julio [FJ 2º].

[258] (STC 115/2013 [FJ 5º] y STC 173/2011 [FJ 2º] entre otras).

constatación ex post de la falta del presupuesto habilitante o del respeto al principio de proporcionalidad implicaría la vulneración del derecho fundamental y tendría efectos procesales en cuanto a la ilicitud de la prueba en su caso obtenida, por haberlo sido con vulneración de derechos fundamentales" (STC 206/2007, de 24 de septiembre y STC 70/2001, de 3 de abril)[259]. En definitiva prevalece el respeto al principio de proporcionalidad, concretado a su vez en tres condiciones: idoneidad, necesidad y proporcionalidad en sentido estricto.

En este mismo orden de cosas, no se violenta el derecho a la intimidad, porque la Policía haya practicado sin autorización judicial el examen de la agenda telefónica de quien acaba de ser detenido, pues dicha actuación se revela como una acción prudente, razonable y proporcionada, atendidas las circunstancias, como una excepción a la regla general de la necesidad de mandato judicial para invadir la esfera de la intimidad de la persona, siempre que concurran los consabidos requisitos relativos al juicio de idoneidad, de necesidad y de proporcionalidad *estricto sensu* (véanse las SSTC 207/1996, de 16 de diciembre, 70/2001 de 3 de abril de 2002 y 115/2013, de 9 de mayo)[260].

---

[259] *En el caso concreto de la STC 115/2013, de 9 de mayo, "la intervención en el teléfono móvil resulta urgente por la necesidad de averiguar la identidad de alguna de las personas que huyeron al ser sorprendidas in fraganti custodiando un alijo de droga, para proceder a su detención de tal manera que no se sustrajeran definitivamente a la acción de la justicia".*

[260] Resulta interesante analizar cómo la STC 115/2013 aplica estos presupuestos al específico supuesto al que se refiere:
a) Idoneidad de la medida: "con el acceso policial a las agendas de contactos telefónicos de los terminales móviles incautados en el lugar de los hechos, acceso que se limitó a los datos recogidos en dichas agendas, sin afectar a los registros de llamadas, y que no necesitó de ningún tipo de manipulación extraordinaria por parte de los agentes policiales, toda vez que para acceder a las funciones de los terminales móviles no fue necesario introducir contraseña o clave de identificación personal alguna, al hallarse encendidos los teléfonos móviles, se consiguió identificar como usuario de uno de dichos aparatos, y a la postre detener, al recurrente".
b) Necesidad de la medida: "no existía otra medida más moderada para la consecución de tal propósito la identificación de las personas que huyeron tras ser sorprendidas por la policía en el invernadero donde fue aprehendido el alijo de droga con igual eficacia, toda vez que gracias a la identificación inmediata del recurrente como usuario de uno de los teléfonos móviles encontrados por los agentes de policía se pudo corroborar su presencia en el lugar de los hechos, así como obtener otras pruebas incriminatorias para fundamentar la convicción judicial sobre su participación en el delito contra la salud pública por el que ha sido condenado".
c) Juicio de proporcionalidad en sentido estricto: "se trató de una medida ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto, dada la naturaleza y gravedad del delito investigado y la leve injerencia que comporta en el derecho a la intimidad del recurrente el examen de la agenda de contactos de su teléfono móvil".

En el mismo sentido se ha pronunciado el Tribunal Supremo[261], al considerar que la agenda de un teléfono móvil, entendiendo por agenda el archivo del aparato en el que consta un listado de números identificados normalmente por un nombre, es equiparable a una agenda en soporte de papel o electrónica con el mismo contenido de direcciones y números de teléfono. Por ello su registro u observación no supone la inmisión o injerencia en el derecho al secreto de las comunicaciones sino en el derecho a la intimidad, con las importantes consecuencias que de ello se derivan. Pues así como la injerencia en el primero de tales derechos requeriría, sin duda ni excepción, la previa autorización judicial, por venir así expresamente dispuesto en el artículo 18.3 de nuestra Constitución, la diligencia que afecta a la intimidad del investigado se encuentra, en cambio, legalmente autorizada a las fuerzas del orden, siempre por supuesto que la misma resulte justificada con arreglo a los criterios de urgencia y necesidad y que se cumpla el requisito de proporcionalidad al ponderar los intereses en juego en el caso concreto[262].

Ahora bien, la LECrim establece de forma precisa y detallada qué medidas de investigación tecnológica se pueden practicar por la Policía sin autorización judicial (art. 588 quinquies b apartado 4º, art. 588 sexies c apartado 3º y 4º). Esta nueva regulación es acorde con la anterior doctrina jurisprudencial relativa la posible vulneración de derechos fundamentales derivada de actuaciones de la policía judicial

[261] SSTS 663/2011, de 7 de julio; 321/ 2011, de 26 de abril; 104/2011, de 1 de marzo; 1315/2009 de 18 de diciembre, 449/2006, de 17 de julio; 1231/2003 de 25 de septiembre; 1086/2003 de 25 de julio; 1235/2002 de 27 de junio, 316/2000 de 3 de marzo, relativas al conocimiento por los agentes policiales de los listados telefónicos de las agendas de teléfonos móviles.

[262] La STS 444/2014, de 9 de junio recuerda que "conviene hacer referencia a la STC (Pleno) 115/2013, de 9 de mayo, que se refiere al acceso por parte de los agentes de la Policía Nacional, sin consentimiento del afectado y sin autorización judicial, a la relación de números telefónicos contenidos en la agenda de contactos telefónicos de un teléfono móvil (entendiendo exclusivamente por agenda el archivo del teléfono móvil en el que consta un listado de números identificados mediante un nombre) que fue encontrado por los agentes en el lugar de comisión de un delito, y considera que esta actuación no afecta al derecho al secreto de las comunicaciones (art. 18.3 CE) del usuario de dicho aparato de telefonía, sino exclusivamente al derecho a la intimidad (art. 18.1 CE) "(...)*con el acceso a la agenda de contactos del teléfono móvil los agentes de policía no obtienen dato alguno concerniente a un proceso de comunicación emitida o recibida mediante dicho aparato, sino únicamente un listado de números de teléfono introducidos voluntariamente por el usuario del terminal, equiparable a los recogidos en una agenda de teléfonos en soporte de papel, por lo que debe descartarse que el derecho al secreto de las comunicaciones quede afectado por esta actuación policial.*
Distinto sería el caso si se hubiese producido el acceso policial a cualquier otra función del teléfono móvil que pudiera desvelar procesos comunicativos, como por ejemplo el acceso al registro de llamadas entrantes y salientes".

relacionadas con exámenes de teléfonos móviles, agendas electrónicas o dispositivos de almacenamiento en el momento de la detención de los sospechosos.

Lo fundamental para considerar válida esta actuación, realizada al margen de la autorización judicial es su naturaleza excepcional, pues en estos casos "*han de acreditarse razones de urgencia y necesidad que hagan imprescindible la intervención inmediata y respetarse estrictamente los principios de proporcionalidad y razonabilidad"* (STS 864/2015, de 10 de diciembre de 2015 y STC 206/2007, de 24 de septiembre).

Esta posibilidad excepcional se reserva a los casos en los que sea materialmente imposible la obtención de la autorización por producirse los hechos fuera del horario de atención del Juzgado o incluso para el caso de que solicitada el Juzgado no se pronuncie en un plazo adecuado a dicha necesidad, debiendo constar en el atestado los datos que permitan comprobar la urgencia y necesidad para el buen fin de la investigación, que serán presupuestos de la validez de la diligencia; igualmente en la resolución que se convalide la medida de investigación, deben cumplirse los requisitos expuestos con carácter previo en cuanto a la solicitud y resolución motivada.

Habrá que atender al caso concreto para ponderar los elementos concurrentes y concluir si la actuación policial es correcta. En caso contrario la consecuencia sería la nulidad de la prueba, al haberse obtenido vulnerando derechos fundamentales[263].

[263] Interesante es la STS 204/2016, de 10 de marzo, en la que se analiza la doctrina jurisprudencial del TS y TC, relacionándolos con la reforma de la LECrim, en concreto los arts 588 sexies que regulan el registro de dispositivos de almacenamiento masivo, en un supuesto en el que la policía accedió a los teléfonos móviles de los detenidos, sin autorización judicial, extrayendo datos de la agenda que llevó a la identificación del receptor de la droga. La sentencia acoge dos motivos del recurso y considera que la prueba de cargo procedente de la injerencia policial en el derecho constitucional a la intimidad sin la concurrencia de razones de urgencia y necesidad que hiciese imprescindible la intervención inmediata es nula, y sin ella la prueba de cargo concurrente para justificar la condena del recurrente es notoriamente insuficiente. En el caso concreto, transcurrieron varios días desde la incautación de los teléfonos móviles hasta su manipulación y examen, considerando el TS que deberá haberse puesto a disposición del Juzgado y pedido autorización judicial.

2. SECRETO DE LAS COMUNICACIONES.

2.1 Contenido de la comunicación.

La protección del derecho al secreto de las comunicaciones tiene una entidad propia y diferenciada de su vinculación con el derecho a la intimidad, ya que las comunicaciones deberán resultar protegidas con independencia de su contenido. El derecho fundamental del art. 18.3 CE cubre no sólo el contenido de la comunicación, sino también otros aspectos externos de la misma, como ha venido afirmando el TEDH en las sentencias de 2 de agosto de 1984 (caso *Malone c. Reino Unido)* y de 3 de abril de 2007 (caso *Copland c. Reino Unido*) así como el propio TC español.

Nuestra jurisprudencia establece[264] que el artículo 18.3 CE tiene un contenido puramente formal, que protege tanto de las intromisiones de los poderes públicos como de los particulares[265]. Siguiendo la jurisprudencia del Tribunal Constitucional, el 18.3 de la CE consagra la libertad de las comunicaciones y garantiza su secreto, sea cual fuere la forma de interceptación, mientras dure el proceso de comunicación, en el marco de comunicaciones indirectas, y frente a terceros ajenos a la comunicación[266]. En este sentido, el secreto de la comunicación se vulnera no sólo con la interceptación de la misma, sino también con el simple conocimiento antijurídico de lo comunicado.

Aunque el artículo 18.3 CE menciona expresamente, las comunicaciones postales, telegráficas o telefónicas, dado el carácter abierto de su enunciado, se entienden comprendidas también otro tipo de comunicaciones como pueda ser el correo electrónico, chats o mensajería instantánea, u otros medios en los que se use algún artificio instrumental o técnico[267] y la presencia de un elemento ajeno a aquéllos entre

[264] SSTC 114/1984, de 29 de noviembre; 281/2006, de 9 de octubre; SSTS 208/2006, de 20 de febrero y 309/2015, de 22 de mayo.

[265] STC 123/2002, de 20 de mayo "*En una sociedad tecnológicamente avanzada como la actual, el secreto de las comunicaciones constituye no sólo garantía de libertad individual, sino instrumento de desarrollo cultural, científico y tecnológico colectivo*".

[266] SSTC 114/1984, de 29 de noviembre; 49/1999, 5 de abril; 70/2002, 3 de abril; 184/2003, de 23 de octubre y 281/2006, de 9 de octubre

[267] GONZÁLEZ PÉREZ, J. J. Utilización en el proceso penal de datos vinculados a las comunicaciones electrónicas recopilados sin indicios de comisión delictiva en "Protección de datos y proceso penal". Ed.

los que media el proceso de comunicación es indispensable para configurar el ilícito constitucional del precepto. En consecuencia, el levantamiento del secreto por uno de los intervinientes no se consideraría violación del artículo 18.3 CE, sino, en su caso, vulneración del derecho a la intimidad[268].

Además, el secreto cubre tanto el contenido de la comunicación como la identidad subjetiva de los interlocutores[269], por lo que queda afectado por este derecho tanto la entrega de los listados de llamadas telefónicas por las compañías telefónicas como también el acceso al registro de llamadas entrantes y salientes grabadas en un teléfono móvil[270]. Asimismo, el acceso a determinados datos o aspectos externos de la comunicación que pueden encontrarse en el propio dispositivo electrónico (como ocurre con los registros almacenados en archivos temporales) también se encuentra amparado por el derecho fundamental al secreto de las comunicaciones.

Igualmente, en las comunicaciones a través de dispositivos electrónicos puede afirmarse que el derecho fundamental al secreto de las comunicaciones ampara también los datos que acompañan al proceso de comunicación; esto es, *cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente*[271].

La protección de este tipo de comunicaciones supone que no podrá interferirse o intervenirse la comunicación de cualquier persona salvo resolución judicial y con las garantías previstas. Al existir una reserva jurisdiccional, es siempre exigible la previa autorización judicial con los requisitos ya examinados.

La Ley, 2010, pág. 356 se refiere a las comunicaciones telemáticas como los servicios de comunicación que permite Internet, incluyendo el correo electrónico; la mensajería instantánea (servicio IRC, servicio ICQ, la voz sobre IP-VoIP, la videoconferencia y el envío de archivos en muchas ocasiones tipo P2P); los foros y blogs; y la navegación a través de internet.

[268] STC 114/1984, de 29 de noviembre [FJ 7º].

[269] STC 114/1984, de 29 de noviembre [FJ 7º]; STC 123/2002, de 20 de mayo [FJ 3º]; STC 56/2003, de 24 de marzo [FJ 2º]; STC 230/2007, de 5 de noviembre [FJ 2º].

[270] STC 142/2012 de 2 de julio [FJ 2º] y STC 230/2007 de 5 de noviembre. [FJ 2º].

[271] Definición de datos sobre el tráfico contenida en el art. 1 d) Convenio sobre Ciberdelincuencia de Budapest

La mayor incidencia del derecho garantizado por el art. 18.3 CE la encontramos en las comunicaciones telefónicas/telemáticas, donde se plantean distintos grados de posible vulneración del secreto: intervención, grabación o recuento (STC 217/1989, de 21 de diciembre). Es decir, se admite la vulneración del derecho no sólo cuando se accede a lo comunicado, sino también cuando se conoce con quién o con qué número se comunica, e incluso la duración de la comunicación, según ha puesto de relieve el TEDH (Sentencia de 30 de julio de 1998, caso Valenzuela Contreras contra España) o el Tribunal Constitucional, el cual, no obstante ha destacado "la menor intensidad de la injerencia" cuando no se accede al contenido de la comunicación (STC 123/2002, de 20 de mayo).

En todo lo relativo a las comunicaciones telefónicas/telemáticas ha sido clave la jurisprudencia desarrollada por el Tribunal Europeo de Derechos Humanos, al destacar la necesidad de que la interceptación esté prevista mediante ley, que resultara accesible al justiciable y predecible, y que sería necesaria en una sociedad democrática (Sentencias de 25 de marzo de 1998, caso *Kopp c. Suiza*, y de 28 de septiembre de 2000, caso *Messina c. Italia,* entre otras) así como la exigencia de proporcionalidad (Sentencia de 20 de junio de 2000, caso *Foxley c. Reino Unido*).

La atención del TEDH se ha centrado también en precisar que la vigilancia puede sufrir un control en tres estadios:

1º) Cuando se ordena.

2º) Mientras se lleva a cabo.

3º) Cuando ha cesado.

Estos tres estadios podrán ser sometidos a control por parte del poder judicial (STEDH de 6 de septiembre de 1978, asunto *Klass y otros c. Alemania*).

De la jurisprudencia del TEDH, tres resoluciones han tenido una especial incidencia para España, la del caso Valenzuela Contreras (Sentencia de 30 de julio de 1998), la del asunto Prado Bugallo (Sentencia de 18 de febrero de 2003) y la de Abdulkadir Coban contra España (Decisión de 26 de septiembre de 2006). En la primera se pusieron de relieve las deficiencias de la regulación española anteriores a la L.O.

4/1988; en la segunda, si bien se apreciaron favorablemente los cambios introducidos, se estimó que aun resultaba insuficiente la determinación de la naturaleza de las infracciones para dar lugar a las intervenciones, la fijación de los límites temporales y de las condiciones de aportación de la prueba al juicio oral[272]. En la tercera, se matizan los requisitos para intervenir las comunicaciones.

De las observaciones del TEDH en el asunto Valenzuela se hicieron eco tanto la jurisprudencia del Tribunal Supremo (entre otras, STS 2ª de 22 de noviembre de 1999) como la constitucional (véase, por todas, STC 202/2001, de 21 de noviembre), hasta que finalmente ha quedado resuelta la cuestión tras haber sido tratada la intervención de las comunicaciones con la suficiente precisión por el legislador, además de recoger las exigencias del Convenio sobre Ciberdelincuencia respecto a los nuevos medios de investigación tecnológica. Así, la regulación legal de las intervenciones telefónicas y telemáticas la encontramos en el art. 588 ter LECrim.

[272] Entre los requisitos que había precisado la jurisprudencia cabe destacar: en primer lugar la necesidad de motivación, cuya carencia llevará a la invalidación de, en su caso, las pruebas obtenidas (STC 54/1996, de 26 de marzo). La resolución judicial que autoriza la medida o su prórroga debe expresar o exteriorizar tanto las razones fácticas como jurídicas que apoyan la necesidad de la intervención. Deberá precisarse con la mayor certeza posible el objeto de la medida: número o números de teléfono y personas cuyas conversaciones han de ser intervenidas con determinación del grado de intervención, el tiempo de duración de la intervención (que revestirá un carácter razonable), quiénes han de llevarla a cabo y cómo, y los periodos en los que deba de darse cuenta al juez de sus resultados para controlar su ejecución (STC 202/2001 de 15 de octubre; STS 2145/2002 de 16 de diciembre; ATS de 18 de junio de 1992). Siempre partiendo de la existencia de unas sospechas que "han de fundarse en datos fácticos o indicios que permitan suponer que alguien intenta cometer, está cometiendo o ha cometido una infracción grave o en buenas razones o fuertes presunciones de que las infracciones están a punto de cometerse" (STC 202/2001, de 15 de octubre). Las condiciones de legitimidad de la limitación del derecho al secreto de las comunicaciones afectan también a las resoluciones de prórroga, de tal forma que no sólo necesitarán también de motivación, que no podrá ser mera reproducción de la primera, sino que se exige que el Juez conozca los resultados de la intervención acordada (resultados, utilidad para el proceso...) (SSTC 49/1999 de 5 de abril; 138/2001, de 18 de junio). Además, se produciría una vulneración del derecho desde el momento en que expirara la orden judicial sin ser renovada (STEDH de 20 de junio de 2000, caso *Foxley*).
Por su parte, como efecto del caso Prado, donde el TEDH todavía señala deficiencias en nuestro ordenamiento en la regulación de las intervenciones telefónicas, el Tribunal Constitucional en la Sentencia 184/2003 de 23 de octubre, reconocía las carencias del art. 579 LECrim. en lo que respecta al plazo máximo de duración de las intervenciones, la naturaleza y gravedad de los hechos en virtud de cuya investigación pueden acordarse; al control del resultado de las intervenciones telefónicas y de los soportes en los que conste dicho resultado, a las condiciones de incorporación a los atestados y al proceso de las conversaciones intervenidas. Por estas y otras razones el Alto Tribunal concluía que no se ajustaba a las exigencias de previsibilidad y certeza en el ámbito del derecho fundamental al secreto de las comunicaciones, por lo que instaba al legislador para que en el plazo más breve posible regule con la suficiente precisión esta materia.

2.2 Fases del proceso de comunicación a través de una red[273].

El proceso de comunicación a través de una red presenta distintas fases, existiendo supuestos en los que el contenido material queda almacenado en los servidores una vez concluida su transmisión al receptor. Como punto de partida hay tener presente que en el proceso de comunicación se distinguen tres momentos:

1º) la transmisión

2º) el almacenamiento del correo en el servidor del receptor

3º) el acceso del receptor al mensaje.

Por otra parte, se trata de comunicaciones cuyo objeto es la recepción por el destinatario de una determinada información, distintas de aquéllas en las que existe una conversación o comunicación recíproca simultánea, por lo que la transmisión concluye cuando el destinatario accede al contenido (material) de la comunicación y no cuando recibe la comunicación.

Para profundizar en este análisis cabe distinguir tres grupos de supuestos:

a) En primer lugar, nos encontramos con aquellos casos en los que no está presente ningún proceso de comunicación. El mero acceso a la información de dispositivos electrónicos en los que no concurra un proceso de comunicación no afecta al secreto de las comunicaciones y sí al derecho a la intimidad. Por ejemplo, la STS 691/2009, de 5 de junio, que se refiere a la información contenida en un CD que ha sido incautado en una entrada y registro, señala que no resulta afectado el derecho al secreto de las comunicaciones, argumentando que *un CD puede, como soporte físico, contener una comunicación postal; pero la protección de la norma constitucional no alcanza al objeto físico como continente o soporte, si no contiene tal comunicación entre dos personas.* En estos supuestos no se encuentra afectado en derecho fundamental al secreto de las comunicaciones, sin perjuicio de la afectación al derecho a la intimidad.

[273] DELGADO MARTIN, J. Derechos fundamentales afectados en el acceso al (…) ob. cit. pág 1-20.

b) En segundo término, podemos situar aquellos supuestos en los que concurre con claridad un proceso de comunicación en curso, por lo que se produce una clara afectación del derecho al secreto de las comunicaciones. Concurre en dos casos: cuando se accede al contenido de un mensaje o correo que ha sido enviado y recibido, pero que todavía no ha sido leído por el destinatario, y cuando el mismo se encuentra en proceso de transferencia.

c) En tercer lugar, hay ocasiones en las que está presente un proceso de comunicación terminado o consumado, o aún no iniciado, que concurre en los siguientes supuestos: acceso al contenido de un mensaje que no ha sido enviado; y, por otra parte, cuando el mismo ha sido enviado, recibido y leído, encontrándose almacenado en el dispositivo electrónico (o en su caso en el servidor).

En principio puede pensarse que estos supuestos únicamente afectan al derecho a la intimidad; la STS 785/2008, de 25 de noviembre, hace referencia a un supuesto en el que las evidencias de la comisión del delito de posesión y difusión de pornografía infantil (conversaciones de chat que revelan que el acusado participaba como parte activa en el intercambio de archivos, ficheros y documentos de contenido pornográfico infantil), se encontraban almacenadas en los equipos informáticos intervenidos en una diligencia de entrada y registro. Entiende la Sentencia que en este caso *se trataba de unas comunicaciones por internet, ya celebradas y concluidas, de tal suerte que sólo constituía material de archivo,* por lo que no considera afectado el derecho fundamental al secreto de las comunicaciones. Sin embargo, como acertadamente se ha dicho[274] esta solución, no está exenta de dificultades prácticas. De esta manera, se razona que, *de ordinario, en cualquier programa de gestión de correo electrónico se agolpan mensajes recibidos y abiertos, no abiertos y eliminados sin abrir. Si bien se mira, la elección del régimen jurídico que va a legitimar el acto jurisdiccional de injerencia no puede hacerse depender del momento en el que se halla el proceso de comunicación cuando éste, por la misma realidad de las cosas, se desconoce ex ante. La investigación puede poner de manifiesto la existencia de una cuenta de correo desde la que se envían y reciben mensajes de interés para el seguimiento de los imputados.* Por ello, se concluye que *resultará mucho más seguro estimar que el acceso a esos mensajes, ya sean los que se hallen en el servidor pendientes de descarga como los que se encuentren*

[274]MARCHENA GÓMEZ, M. "Dimensión jurídico-penal del correo electrónico". ob. cit. pág. 18

almacenados en el ordenador del sospechoso, abiertos o no, requiere una resolución jurisdiccional ajustada a las exigencias constitucionales y legales que legitiman la injerencia en el secreto de las comunicaciones"[275].

Es ésta, en definitiva, la interpretación más favorable para la garantía de los derechos fundamentales en presencia y, en concreto, el secreto de las comunicaciones[276].

Lo mismo sucede en relación con el registro de llamadas[277]. La relación de llamadas emitidas o recibidas por un terminal telefónico es materia que afecta al derecho que garantiza el art. 18.3 CE, siendo necesario a falta de consentimiento de los sujetos comunicantes, la autorización judicial correspondiente otorgada en el curso de una investigación de carácter penal. Tal autorización será también necesaria para acceder al registro de llamadas entrantes y salientes grabadas en un teléfono móvil (STEDH de 3 de abril de 2007, caso *Copland* contra Reino Unido; STC 142/ 2012, de 2

[275] MARCHENA GÓMEZ, M. "Dimensión jurídico-penal del correo electrónico". ob. cit. pág. 18

[276] SÁNCHEZ SISCART J. M. "A vueltas con el secreto de las comunicaciones: algunos supuestos críticos en la jurisprudencia de la Sala 2ª del Tribunal Supremo" en Diario La Ley nº 7338, Sección Doctrina, 9 de febrero de 2010, entiende que los mensajes abiertos y leídos (por ejemplo, contenidos en la bandeja de correo electrónico, o incluidos en un sobre o envoltorio propio de unacomunicación postal, etc.) no quedan desprovistos, por este mero hecho, de la protección constitucional, pues el derecho al secreto de las comunicaciones cubre también los datos registrados en el momento en el que se está produciendo el proceso de comunicación, aunque se tomen en consideración o se averigüen una vez finalizado el proceso comunicativo.

[277] La STC 230/2007, de 5 de noviembre analiza un supuesto en que los agentes actuantes intervienen en poder de unos detenidos sendos teléfonos móviles, accediendo, entre otros, al registro de llamadas memorizado en el terminal hallado en posesión de uno de ello, sin contar con su consentimiento ni con la debida autorización judicial, confeccionando un listado de llamadas recibidas, enviadas y perdidas. El TC considera que se ha vulnerado al recurrente el derecho al secreto de las comunicaciones en tanto que "*dicho acceso no resulta conforme a la doctrina constitucional reiteradamente expuesta sobre que la identificación de los intervinientes en la comunicación queda cubierta por el secreto de las comunicaciones garantizado por el art. 18.3 CE y, por tanto, que resulta necesario para acceder a dicha información, en defecto de consentimiento del titular del terminal telefónico móvil intervenido, que se recabe la debida autorización judicial. Ello supone la imposibilidad de valoración de dicha prueba al tener que quedar excluida del material probatorio apto para enervar la presunción de inocencia, en tanto que obtenida con vulneración de derechos fundamentales del recurrente".*
Pero es claro que por orden judicial pueden reclamarse los listados de llamadas a las compañías telefónicas (STC 123/2002, de 20 de mayo, STS 1330/2002, de 16 de julio). No tendría sentido alguno que pudieran intervenirse judicialmente las conversaciones que inciden directamente sobre el derecho al secreto de las comunicaciones, y no pudiera por orden judicial solicitarse a la compañía telefónica operadora en cada caso que expidiera tales listados de llamadas, diligencia cuya afectación para el derecho protegido es de menor intensidad.
Además, en tanto la injerencia consistente en la entrega de los listados de las llamadas de una persona por las compañías telefónicas debe considerarse de "menor intensidad" que las escuchas telefónicas, ha de partirse de que este dato es "especialmente significativo en orden a la ponderación de su proporcionalidad".

de julio, STC 230/2007, de 5 de noviembre; STS 513/2010, de 2 de junio, STS 707/2009, de 22 de junio)[278].

2.3 Régimen jurídico del secreto a las comunicaciones.

La regulación legal de las intervenciones telefónicas y telemáticas se encuentra hoy en el art. 588 ter LECrim y la detención y apertura de la correspondencia escrita y telegráfica en el capítulo III del Título VIII de la LECrim añadido por el artículo 10 de la Ley Orgánica 13/2015, de 5 de octubre (artículos 579 a 588).

Estas normas delimitan el contenido esencial del art. 18.3 CE, es decir, desarrollan los criterios de intervención judicial de las comunicaciones telefónicas, telemáticas[279], postales y telegráficas. La LECrim ha estimado oportuna la proclamación normativa de los principios que el Tribunal Constitucional ha definido como determinantes de la validez del acto de injerencia (especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida) y condiciona la autorización judicial[280] a que se trate de determinados delitos.

Las dudas acerca de si el correo electrónico debía ser considerado como correspondencia postal han quedado resueltas, pues ahora la LECrim regula conjuntamente la intervención de las comunicaciones de cualquier clase que se realicen a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual. Será el propio juez, ponderando la gravedad del hecho que está siendo objeto de investigación, quien determine el alcance de la injerencia del Estado en las comunicaciones particulares y tendrá que motivar, a la luz de aquellos principios, si el sacrificio de las comunicaciones telefónicas no es suficiente y si la investigación exige,

[278] Circular de la Fiscalía General del Estado 1/2013 sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas.

[279] proyectando estas condiciones al correo electrónico por considerarse un medio asimilable al teléfono. ZOCO ZABALA, C. "Interceptación de las comunicaciones electrónicas". Concordancias y discordancias de SITEL con el artículo 18 CE. In Dret, revista para el análisis del derecho. Barcelona, octubre 2010. http://www.indret.com/pdf/781_es.pdf

[280] SSTC 5/2010, de 7 de abril; 220/2009 de 21 de diciembre; 26/2006 de 30 de enero y 253/2006, de 11 de septiembre.

además, la interceptación de los SMS, MMS, correo electrónico o cualquier otra forma de comunicación telemática de carácter bidireccional[281].

3. EL DERECHO A LA PROTECCIÓN DE DATOS .

La protección de los datos frente al uso de la informática se encuentra regulada en el artículo 18. 4 de nuestra Constitución[282].

Una primera interpretación llevó a considerar este derecho como una especificidad del derecho a la intimidad, aunque el Tribunal Constitucional considera que el derecho fundamental a la protección de datos personales (arts. 10 y 18.4 CE) es un derecho independiente, pero estrechamente relacionado con aquél[283]; es un derecho autónomo que faculta a la persona a controlar sus datos personales y la capacidad para disponer y decidir sobre los mismos[284].

Aunque el Alto Tribunal estableció la vinculación directa de este derecho para los poderes públicos sin necesidad de desarrollo normativo[285], se encuentra desarrollado por la Ley Orgánica de Protección de Datos Personales 15/1999 de 13 de diciembre[286].

---

[281] RODRÍGUEZ LAINZ, J. L. "Reflexiones sobre los nuevos contornos del secreto de las comunicaciones (Comentario a la STC 170/2013, de 7 de octubre)". Diario La Ley nº 8271, 2014.

[282] Art. 18.4 CE "*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"*.
La Constitución Española fue una de las primeras en introducir este artículo dado que es precisamente en los años de su redacción cuando comienzan a apreciarse los peligros que puede entrañar el archivo y uso ilimitado de los datos informáticos. Nuestros constituyentes tomaron, en este caso, el ejemplo de la Constitución portuguesa, sólo dos años anterior a la española.

[283] STC 254/1993, de 20 de julio y STC 290/2000, de 30 de noviembre.

[284] La STC 94/1998, de 4 de mayo señaló que "*nos encontramos ante un derecho fundamental a la protección de datos por el que se garantiza a la persona el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados; de esta forma, el derecho a la protección de datos se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquél que justificó su obtención"*.

[285] STC 254/1993, de 20 de julio [FJ 6º].

[286] El desarrollo del derecho está marcado por el Convenio del Consejo de Europa de 28 de enero de 1981, para la protección de datos de carácter personal. La primera regulación interna produjo con la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal (LORTAD)vino impuesta por la ratificación por parte de España del Convenio de Schengen,

Mediante la protección de este derecho se intenta lograr la adecuación y exactitud de las bases de datos y la cancelación cuando dejen de ser necesarios, así como el conocimiento y la posibilidad de acceso por parte de los afectados, con un especial deber de protección para los datos denominados sensibles, aquellos que afectan a la ideología, religión o creencias (art. 16.2 CE) y los relativos a la salud[287].

La protección de datos no alude sólo a la reserva con la que se han de tratar ciertas informaciones, sino que viene fundamentalmente caracterizada por el reconocimiento a todos los ciudadanos de un poder de control sobre sus propios datos, en todo momento y dondequiera se encuentren. Ello permite hablar de un poder de control que desde el punto de vista activo tiene un carácter individualizado, pero también difuso, y desde el punto de vista pasivo va dirigido frente a todos aquellos sujetos que disponen de datos de carácter personal[288].

En la doctrina española, PÉREZ GIL sostiene que la fase de investigación del proceso penal constituye una continuada intromisión en el ámbito de tutela que propicia

---

donde para permitir el libre paso de fronteras entre diversos países europeos imponía el control de ciertas bases de datos. La Directiva 95/46/CE, del Parlamento europeo y del Consejo de 24 de octubre de 1995, sobre protección de datos y libre circulación de esos datos (DOCE L 281, de 23 de noviembre de 1995), dio lugar a la redacción de una nueva ley, la L.O.15/1999 de 13 de diciembre, de protección de datos de carácter personal y su reglamento Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
En la actualidad, en el ámbito europeo hay que resaltar el Reglamento Europeo de Protección de datos, por el que se deroga a la Directiva 95/46/CE (Reglamento General de Protección de datos), que constituye la norma fundamental de la Unión Europea en materia de protección de datos personales y de la libre circulación de los datos aplicable al territorio de la UE y a sus ciudadanos. Es una norma de efecto directo que no requiere transposición al derecho interno, y que armoniza las legislaciones existentes hasta ahora en los Estados Miembros. Entró en vigor el 26 de mayo de 2016 y será de aplicación a partir del 25 de mayo de 2018.

[287] Este derecho se halla estrechamente vinculado con la libertad ideológica, pues evidentemente el almacenamiento y la utilización de datos informáticos puede suponer un riesgo para aquélla, no solamente por lo que se refiere a 'datos sensibles', entre los que se encuentran los de carácter ideológico o religioso sobre los cuales según indica el artículo 16 de la Constitución nadie estará obligado a declarar, sino también por su posible utilización ajena a las finalidades para los que fueron recabados (SSTC 11/1998, de 13 de enero; 44 y 45/1999, de 22 de marzo, entre otras, en relación con la libertad sindical), o la inclusión de datos sin conocimiento del afectado (STC 202/1999, de 8 de noviembre). Otro riesgo puede provenir por efectuarse accesos indebidos a ficheros ajenos (STC 144/1999, de 22 de julio, en torno a una indebida utilización por parte de una Junta Electoral de Zona de datos incluidos en el Registro Central de Penados y Rebeldes). Además, la Ley regula el régimen de creación, modificación o supresión de ficheros informáticos, así como de su cesión. Crea la Agencia de Protección de Datos, con el fin de velar por el cumplimiento de la ley y el Registro General de Protección de Datos en el que deberán inscribirse todos los ficheros de acuerdo con la Ley. Por último, establece un régimen sancionador.

[288] PÉREZ GIL, J. "Investigación penal y nuevas tecnologías: algunos de los retos pendientes." Revista jurídica de Castilla y León nº 7, Octubre 2005, pág. 228.

toda la normativa de protección de datos personales, y critica que el acceso a datos personales por parte de la policía y su tratamiento, sea una actividad que integra hoy habitualmente sus funciones, pues constituye una forma de actuación completamente al margen de la actividad jurisdiccional (y ni siquiera de la del Ministerio Fiscal)[289].

Defiende también que ni siquiera nuestro TS otorga la relevancia requerida a la materia que nos ocupa, tal y como acredita la copiosa jurisprudencia relativa a peticiones de registros y listados de llamadas, pues aun admitiendo que no afectan al secreto de las comunicaciones, tales listados pueden contener datos de carácter personal. Pero el Alto Tribunal suele considerar bastante una providencia sin motivación alguna para acordar su solicitud, o no delimita con la suficiente nitidez conceptos esenciales de la normativa de protección de datos que sin embargo entiende de aplicación[290]. Una cosa es que no nos hallemos en el ámbito del art. 18.3 CE, pero otra muy diferente es sostener que en absoluto estemos ante un derecho fundamental a fin de excluir del monopolio jurisdiccional la adopción y control de aquellas medidas que pudieran vulnerarlo o devaluarlo[291].

Esa misma línea del Tribunal Supremo ha sido acogida por la LECrim[292], por cuanto no se exige a la policía autorización judicial para la identificación de titulares o

[289] PÉREZ GIL, J. "Investigación penal y nuevas tecnologías (…) ob. cit. pág. 228.

[290] STS 1219/2004, de 10 de diciembre [FJ 16]. Un dictamen de la Agencia de Protección de Datos fechado en 1999 vino a convalidar la idoneidad de las solicitudes de datos efectuadas por la Policía Judicial sin mandamiento judicial o requerimiento previo del Ministerio Fiscal, un fundamento al que todavía hoy se siguen aferrando los cuerpos policiales en sus requerimientos de aportación de datos.

[291] PÉREZ GIL, J. "Investigación penal y nuevas tecnologías (…) ob. cit. pág. 229. La jurisprudencia de la Sala 2ª sobre listados de llamadas es abundantísima en los últimos tiempos: STS 23/2005, de 21 de enero; STS 1219/2004, de 10 de diciembre; STS 1167/2004, de 22 de octubre; STS 889/2004, de 9 de julio; STS 1683/2003, de 11 de diciembre; STS 769/2003, de 31 de mayo. Acorde con el derecho fundamental a la intimidad en el supuesto de recabar listado de llamadas parece STS 769/2003, de 31 de mayo al hacer constar que *"Lo cierto es que, por sus especiales características, afectaba al derecho a la intimidad del denunciante y ofendido por el delito, por lo que la actitud inicial, observada por el Juez de Instrucción, al solicitar la entrega voluntaria de los datos, fue absolutamente correcta y respetuosa con el derecho fundamental afectado".* El ejemplo nos lo proporciona la STS 1167/2004, de 22 de octubre, en la que no se distinguen los requisitos del consentimiento para el tratamiento (art. 6.2 LOPD, innecesario cuando es tratamiento de datos personales por las administraciones) de los del consentimiento para la cesión (11.2.d, en el que se habla únicamente del Ministerio Fiscal y los Jueces o Tribunales, pero que no se refiere a la Policía).

[292] Art. 588 ter m "*Cuando, en el ejercicio de sus funciones, el Ministerio Fiscal o la Policía Judicial necesiten conocer la titularidad de un número de teléfono o de cualquier otro medio de comunicación, o, en sentido inverso, precisen el número de teléfono los datos identificativos de cualquier medio de comunicación, podrán dirigirse directamente a los prestadores de servicios de telecomunicaciones, de*

terminales o dispositivos de conectividad, pudiendo ser dirigidas las solicitudes directamente a las Empresas Proveedoras de Servicios apercibiéndolas de desobediencia.

Otro interesante problema[293] se refiere a si los datos obtenidos para investigar un concreto hecho delictivo podían ser utilizados, sin previa autorización judicial, para la investigación de otras infracciones penales, o ser usados para la llamada búsqueda entrecruzada de rasgos distintivos (es decir, para comparar automatizadamente los datos de personas que tienen determinadas características coincidentes con las del presunto autor del delito con la finalidad de centrar las pesquisas en determinados sujetos). Tal cuestión ha quedado resuelta en LECrim pues exige que se solicite del juez competente autorización para recabar la información que conste en los archivos automatizados de los prestadores de servicios, incluida la búsqueda entrecruzada o inteligente de datos, siempre que se precisen la naturaleza de los datos que hayan de ser conocidos y las razones que justifican la cesión.

Por último, la LECrim, consciente del problema que suponía para el derecho a la protección de datos y para el derecho a la intimidad, el destino de todo el material electrónico usado en la investigación cuando ya no es imprescindible o es irrelevante para la investigación, ha dispuesto, una vez que se ponga término al procedimiento mediante resolución firme, el borrado y eliminación de los registros originales que puedan constar en los sistemas electrónicos e informáticos utilizados en la ejecución de la medida, conservándose una copia por el Letrado de la Administración de Justicia que será destruida a los cinco años desde que la pena se haya ejecutado o cuando el delito o la pena hayan prescrito o se haya decretado el sobreseimiento libre o haya recaído sentencia absolutoria firme respecto del investigado, dictando los Tribunales las órdenes oportunas a la Policía Judicial para que lleve a efecto la destrucción (artículo 588 bis k. Destrucción de registros).

4. EL DENOMINADO "DERECHO A LA IDENTIDAD VIRTUAL."

acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, quienes estarán obligados a cumplir el requerimiento, bajo apercibimiento de incurrir en el delito de desobediencia."

[293] DELGADO MARTIN, J, "Derechos fundamentales afectados en el acceso al (…) ob. cit. pág 13.

En estos últimos años se viene afirmando por parte de algunos autores la existencia de un nuevo derecho a "la identidad virtual", nacido precisamente del uso de las nuevas tecnologías[294].

Este nuevo derecho, cuyo germen doctrinal puede encontrarse en la STC 173/2011, de 7 de noviembre, abarcaría una serie de elementos comunes del derecho a la intimidad, secreto de las comunicaciones y del derecho de protección de datos personales. Se fundamenta en la consideración de que los datos obtenidos de la interactuación de una persona a través de las nuevas tecnologías, individualmente considerados o estudiados, no revelan ningún aspecto íntimo de la misma, pero si son estudiados en su conjunto, una vez analizados, pueden llegar a describir aspectos realmente relevantes de la personalidad de su titular[295].

No se puede tratar al ordenador y en general, a los dispositivos tecnológicos de almacenamiento de información, como si fueran una pieza de convicción más, pues en ellos coexisten datos técnicos y datos personales susceptibles de protección constitucional en el ámbito del derecho a la intimidad y la protección de datos (art. 18.1 y 4 de la CE). Pero su contenido también puede albergar información esencialmente ligada al derecho a la inviolabilidad de las comunicaciones (art. 18.3), como es el correo electrónico, que cuando es leído por su destinatario está amparado por el derecho a la intimidad. En este sentido, se afirma el **"derecho al propio entorno virtual"**, integrado por todos esos datos que individualmente considerados, están protegidos por algunos de los derechos fundamentales convergentes antes indicados, pero que precisamente por su

[294] ZARAGOZA TEJADA, J. I., "La reforma operada por Ley 13/2015. El Agente Encubierto Informático".ob. cit. pág 5. VALVERDE MEGÍAS, R., "Intervención de comunicaciones telemáticas y registro remoto".ob.cit. pág. 26 CONDE-PUMPIDO TOURÓN, C. "La reforma procesal. Registro de sistemas informáticos, ampliación del registro a otros sistemas(…) ob. cit. pág. 5.

[295] STC 173/2011, de 7 de noviembre.*"(...) Es evidente que cuando su titular navega por Internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico, forma parte de grupos de noticias, entre otras posibilidades, está revelando datos acerca de su personalidad, que pueden afectar al núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc. Quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona."*

interrelación alrededor de un mismo titular de derechos y datos, precisan de un tratamiento unitario[296].

La ponderación judicial de las razones que justifican en el marco de una investigación penal el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de vista la multifuncionalidad de los datos que se almacenan en dicho dispositivo. Por lo que su tratamiento jurídico puede llegar a ser más adecuado si los mensajes, las imágenes, los documentos y, en general, todos los datos reveladores del perfil personal, reservado o íntimo de cualquier encausado, se contemplan de forma unitaria. Y es que, más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existiría un auténtico derecho al propio entorno virtual. En él se integraría, sin perder su genuina sustantividad como manifestación de derechos constitucionales de *nomen iuris* propio toda "*la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos".* Surge entonces la necesidad de dispensar una

[296]Este criterio ya puede apreciarse en la doctrina jurisprudencial de la Sala Segunda del Tribunal Supremo. Así, en la STS 342/2013, del 17 de abril, se habla expresamente ya del derecho al propio entorno virtual y se justifica en la misma una cita de cierta amplitud: "*El acceso de los poderes públicos al contenido del ordenador de un imputado, no queda legitimado a través de un acto unilateral de las fuerzas y cuerpos de seguridad del Estado. El ordenador y, con carácter general, los dispositivos de almacenamiento masivo, son algo más que una pieza de convicción que, una vez aprehendida, queda expuesta en su integridad al control de los investigadores. El contenido de esta clase de dispositivos no puede degradarse a la simple condición de instrumento recipiendario de una serie de datos con mayor o menor relación con el derecho a la intimidad de su usuario. En el ordenador coexisten, es cierto, datos técnicos y datos personales susceptibles de protección constitucional en el ámbito del derecho a la intimidad y la protección de datos (art. 18.4 de la CE). Pero su contenido también puede albergar información esencialmente ligada al derecho a la inviolabilidad de las comunicaciones. El correo electrónico y los programas de gestión de mensajería instantánea no son sino instrumentos tecnológicos para hacer realidad, en formato telemático, el derecho a la libre comunicación entre dos o más personas. Es opinión generalizada que los mensajes de correo electrónico, una vez descargados desde el servidor, leídos por su destinatario y almacenados en alguna de las bandejas del programa de gestión, dejan de integrarse en el ámbito que sería propio de la inviolabilidad de las comunicaciones. La comunicación ha visto ya culminado su ciclo y la información contenida en el mensaje es, a partir de entonces, susceptible de protección por su relación con el ámbito reservado al derecho a la intimidad, cuya tutela constitucional es evidente, aunque de una intensidad distinta a la reservada para el derecho a la inviolabilidad de las comunicaciones. Por ello deviene necesario establecer una serie de garantías frente a los riesgos que existen para los derechos y libertades públicas, en particular la intimidad personal, a causa del uso indebido de la informática así como de las nuevas tecnologías de la información".*

protección jurisdiccional frente a la necesidad del Estado de invadir ese entorno digital en el ámbito de la investigación de los ciberdelitos[297].

El reconocimiento del "entorno virtual propio", incluso como derecho fundamental de nueva generación, queda plasmado en la STS 204/2016 de 10 de marzo, que al analizar el artículo 588 sexies b LECrim (relativo al registro de dispositivos de almacenamiento masivo de información), dispone que "*el legislador otorga un tratamiento unitario a los datos contenidos en los ordenadores y teléfonos móviles, reveladores del perfil personal del investigado,* ***configurando un derecho constitucional de nueva generación que es el derecho a la protección del propio entorno virtual****"*.

Sea como fuere, lo cierto es que tanto desde la perspectiva unitaria del derecho al entorno virtual propio, como de la perspectiva diversa de las garantías constitucionales exigidas para el sacrificio de los derechos a la inviolabilidad de las comunicaciones y a la intimidad, la intervención de un ordenador para acceder a su contenido exige un acto jurisdiccional habilitante. Y esa autorización no está incluida en la resolución judicial previa para acceder al domicilio en el que aquellos dispositivos se encuentran instalados. De ahí que, ya sea en la misma resolución, ya en otra formalmente diferenciada, el órgano jurisdiccional habrá de exteriorizar en su razonamiento que ha tomado en consideración la necesidad de sacrificar, además del domicilio como sede física en el que se ejerce el derecho a la intimidad personal, aquellos otros derechos que convergen en el momento de la utilización de las nuevas tecnologías.

En definitiva, toda investigación criminal (ya sea en el marco de un proceso penal ya iniciado o en el curso todavía de las diligencias policiales previas a la incoación del procedimiento) relacionada con las nuevas tecnologías, ha de desarrollarse con la máxima cautela y prudencia, y teniendo en cuenta siempre la importante incidencia que estas medidas de investigación puede tener en el contenido esencial de los derechos fundamentales reconocidos en el artículo 18 de la Constitución Española.

[297] En el mismo sentido, SSTS 985/2009, de 13 diciembre; 342/2013, de 17 de abril; 97/2015, de 24 de febrero.

CAPÍTULO SÉPTIMO

TÉCNICAS DE INVESTIGACIÓN DE LOS CIBERDELITOS.

1. LAS NUEVAS TÉCNICAS DE INVESTIGACIÓN TECNOLÓGICA.

Los instrumentos de investigación tradicionales se muestran claramente insuficientes para investigar los ciberdelitos. Nuestra normativa procesal no contaba con una regulación aplicable a muchas de las técnicas de investigación necesarias para el esclarecimiento de conductas ilícitas ligadas al uso de las nuevas tecnologías[298], lo que dificultaba la persecución de esta moderna forma de delincuencia.

Hasta la reforma de 2015, la LECrim no regulaba técnicas específicas para la investigación tecnológica. En razón de ello se suplía la insuficiencia legal mediante la aplicación de disposiciones genéricas de la propia Ley procesal, tales como el artículo 282 y mediante la aplicación analógica de los preceptos que regulaban las

[298] España ha sido uno de los últimos países de Europa en adaptar su legislación procesal a este nuevo entorno informático producido con motivo del auge de las TIC, a diferencia de lo acontecido en otros países europeos, que reformaron expresamente su legislación procesal con el objetivo de cumplir lo establecido en el convenio sobre ciberdelincuencia, y regularon nuevas medidas tecnológicas de investigación. 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 alternativa 2013. http://www.fundacionalternativas.org/public/storage/actividades_descargas/5a687574bb9f245b66286372359596d4.pdf por ejemplo, Bélgica reformó su legislación procesal penal en el año 2000, a través de la Ley de 28 de noviembre de 2000 relativa a la criminalidad informática, para introducir nuevas medidas tecnológicas de investigación. El Reino Unido también adaptó su legislación en el año 2000 a través de la *Regulation of Investigatory Powers Act* (RIPA). En Francia, destacan la Ley de 5 de enero de 1988 sobre el fraude informático, la Ley de 23 de enero de 2006 sobre la lucha contra el terrorismo y la adopción de medidas diferentes a los controles de seguridad y de frontera, y más en particular, el plan de lucha contra los delitos informáticos de 14 de febrero de 2005, sobre medidas urgentes de lucha contra el terrorismo internacional; el Decreto de 16 de agosto de 2005 sobre medidas preventivas de adquisición de los datos personales de las personas que usan los lugares públicos de servicios de telecomunicaciones no supervisado o puntos de acceso a internet mediante tecnología inalámbrica; o la Ley núm. 281, de 20 de noviembre de 2006, sobre las escuchas telefónicas. Y en Italia sobresalen el "Codice della privacy" a través del Decreto legislativo núm. 196 de 30 de junio de 2003; el Decreto Ley núm. 144, de 27 de junio de 2008.

intervenciones telefónicas, entradas y registro en lugares cerrados, registro de papeles y efectos.

La jurisprudencia, que venía interpretando extensivamente el artículo 579 de la LECrim, relativo a la intervención judicial de las comunicaciones postales, telegráficas y telefónicas, con el fin de ampliar su ámbito de aplicación, resultaba ya muy forzada para prestar amparo legal, por ejemplo, a la colocación de micrófonos para grabar las conversaciones directas de los sospechosos o para introducir un troyano en su ordenador[299]. De ahí que, dos circunstancias supusieran un hito decisivo para impulsar la reforma de la LECrim:

1º) De una parte, la declaración de invalidez de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modificó la Directiva 2002/58/CE por parte de la STJUE, Gran Sala, de 8 de abril de 2014 (casos C-293/2012 y C- 594/2012), y su posible afectación a la Ley de conservación de datos española[300].

2º) De otra, la declaración efectuada por la STC 145/2014, de 22 de septiembre[301] al establecer que se vulneraba el derecho fundamental al secreto de las comunicación en la interceptación de las conversaciones del detenido en la celda, aunque se contara con autorización judicial motivada, pues esta autorización judicial carecía de norma legal de cobertura. Ello suscitó la necesidad de una reforma legal pues ante la carencia de una norma de cobertura habilitante no podría practicarse ese tipo de

[299] JIMÉNEZ SEGADO, C y PUCHOL AIGUABELLA, M. "Las medidas de investigación tecnológica limitativas de los derechos a la intimidad, la imagen, el secreto de las comunicaciones y la protección datos". Diario La Ley nº 8676, Sección Doctrina, 7 de enero de 2016, pág. 1.

[300] RODRÍGUEZ LAINZ, J L. "La interceptación de las comunicaciones telefónicas y telemáticas en el Anteproyecto de reforma de la Ley de Enjuiciamiento Criminal de 5 de diciembre de 2014". Diario La Ley nº 8465, año 2015, pág. 1

[301]JIMÉNEZ SEGADO, C y PUCHOL AIGUABELLA, M. "Las medidas de investigación tecnológica limitativas de los derechos (…) ob. cit. pág. 1 "*La sentencia del Tribunal Constitucional 145/2014, de 22 de septiembre, declaró vulnerado el secreto de las comunicaciones del recurrente en amparo, a quien se le grabaron, con autorización judicial, sus conversaciones orales cuando estaba detenido en los calabozos policiales, precisamente por ausencia de habilitación legal. Esta sentencia está sin duda en el origen de la reforma y el mero hecho de la nueva regulación".*

diligencias de investigación, mermando las posibilidades de llegar a esclarecer la verdad en muchos delitos graves[302].

Muchos de los interrogantes planteados en la investigación de los ciberdelitos obtuvieron respuesta en la reforma de la LECrim de octubre de 2015 mediante la regulación expresa de específicas técnicas de investigación tecnológica (*"De las medidas de investigación limitativas de los derechos reconocidos en el art. 18 de la Constitución")*[303]. Dichas medidas son:

a) La interceptación de las comunicaciones telefónicas y telemáticas como vía de investigación criminal de los ilícitos que se cometen a través de la red (artículo 588 ter y siguientes).
b) Captación y grabación de comunicaciones orales abiertas mediante el empleo de dispositivos electrónicos (artículo 588 quarter a y ss)
c) La identificación de equipos o usuarios a partir de una dirección IP (artículo 588 ter k)

[302] Con posterioridad otras Sentencias, como la STS 747/2015 de 19 de noviembre [FJ 4º] parte del mismo presupuesto de declarar la nulidad de la diligencia de instalación de dispositivos electrónicos para la captación y grabación de las conversaciones en el domicilio de los acusados, pese a contar con autorización judicial, aplicando la doctrina de la *sentencia 145/2014, de 22 de septiembre*, en la que se decretó la nulidad de las escuchas practicadas mediante micrófonos instalados en unos calabozos policiales por falta de la habilitación legal para realizarlas.

[303]JIMÉNEZ SEGADO, C y PUCHOL AIGUABELLA, M. "Las medidas de investigación tecnológica limitativas de los derechos (…) ob. cit. pág. 3. "*La reforma incorpora prácticamente el articulado del borrador de Código Procesal Penal de 2013"*.
El Título VIII del Libro II se reorganiza en diez capítulos. Las normas relativas a las entradas y registros domiciliarios se dejan intactas, si bien los arts. 545 a 572 se agrupan en un Capítulo I, con el título "De la entrada y registro en lugar cerrado", y los arts. 573 a 579, en un Capítulo II, con el título "Del registro de libros y papeles". A continuación, el Capítulo III se encarga de la "De la detención y apertura de la correspondencia escrita y telegráfica" (arts. 579 a 588). En el Capítulo IV se regulan las "Disposiciones comunes a la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos" [arts. 588 bis a) a 588 bis k)]. El Capítulo V, "La interceptación de las comunicaciones telefónicas y telemáticas", se divide en tres secciones: Sección 1.a, "Disposiciones generales" [arts. 588 ter a) a 588 ter i)]; Sección 2.a, "Incorporación al proceso de datos electrónicos de tráfico o asociados" (art. 588 ter j); y sección 3.a, "Acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad" [art. 588 ter k) a 588 ter m)]. Los arts. 588 quater a) a 588 quater e) forman el Capítulo VI, "Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos". En el Capítulo VII, "Utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización", se contienen los arts. 588 quinquies a) a 588 quinquies c). El Capítulo VIII, "Registro de dispositivos de almacenamiento masivo de información" está constituido por los arts. 588 sexies a) a 588 sexies c). El Capítulo IX, "Registros remotos sobre equipos informáticos" lo constituyen los arts. 588 septies a) a 588 septies c). Y en el Capítulo X se contemplan una serie de "Medidas de aseguramiento" (arts. 588 octies).

d) Identificación de los terminales mediante captación de códigos de identificación del aparato o de sus componentes (artículo 588 ter l).
e) Identificación de titulares o terminales o dispositivos de conectividad. (artículo 588 ter m).
f) Utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen (artículo 588 quinquies a y ss).
g) El registro de dispositivos informáticos de almacenamiento masivo (artículo 588 sexies a y ss) y el registro remoto de equipos informáticos (artículo 588 septies a y ss).
h) La actuación bajo identidad supuesta en los canales cerrados de comunicación telemática, mediante la regulación del *agente encubierto informático* y para la grabación de imágenes y conversaciones, cuando fuera preciso. En ambos casos, la necesidad de autorización judicial garantiza el pleno respeto del derecho la intimidad y al secreto de las comunicaciones de las personas afectadas (artículos 282 bis apartados 6 y 7).

La adecuación de estas diligencias de investigación tecnológica para la investigación del ciberdelito no significa que no resulten también valiosas en la prevención y persecución de otras infracciones tradicionales[304]. Y al contrario, también en este título se contemplan otras técnicas de nueva regulación, que no son indispensables para la investigación de los ciberdelitos, lo que no quiere decir que no puedan ser de aplicación, ni que no puedan coadyuvar al esclarecimiento de los mismos[305].

A la hora de hacer una exposición clara y concisa de estas técnicas de investigación tecnológica, distingo en un primer momento, y siguiendo el orden lógico de la investigación, las que puede practicar la policía por si misma y que no requieren autorización judicial, de aquellas que sí requieren dicha autorización. Dentro de estas últimas, me referiré primero a todas aquellas que venían practicándose, pese a estar

[304] CABEZUDO RODRÍGUEZ, N. "Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal". Boletín del Ministerio de Justicia nº 2186 año 2016. http://www.mjusticia.gob.es/

[305] Por ejemplo, la utilización de los dispositivos técnicos de seguimiento y localización o la captación de comunicaciones orales mediante el empleo de dispositivos electrónicos.

carentes de regulación en LECrim, amparadas en otras leyes y en la jurisprudencia, para finalmente tratar las que tienen una regulación *ex novo* tras la reforma de la LECrim.

2.TÉCNICAS DE INVESTIGACIÓN TECNOLÓGICA QUE NO PRECISAN AUTORIZACIÓN JUDICIAL.

La reforma de la LECrim de 2015 da un tratamiento jurídico individualizado al acceso por agentes de policía al IMSI, IMEI, dirección IP y otros elementos de identificación de una determinada tarjeta o terminal, en consonancia con una jurisprudencia del Tribunal Supremo ya consolidada sobre esta materia.

2.1 Obtención de una IP.

Es el primer paso para desarrollar cualquier investigación de este tipo. La dirección IP[306] es una etiqueta numérica que identifica a una interfaz (elemento de comunicación/conexión) de un dispositivo (ordenador, móvil, pda, ipad, televión, ebook, consola de videojuegos) dentro de una red que utiliza el protocolo IP (*Internet Protocol*). Las direcciones IP son asignadas por los ISP (*Internet service provider),* compañías proveedoras de acceso a Internet (Telefónica, Jazztel, Orange)[307].

El principio básico es el de que "*no se precisa autorización judicial para conseguir lo que es público"*[308]. El Tribunal Supremo considera que estos datos no se

[306] Las direcciones IP se hacíann con la versión 4 del protocolo IP, que consta de cuatro números separados por puntos, y cada número con un valor que oscila de 0 a 255. Se está implantando la versión 6 del protocolo IP, que consta de 16 números separados por dos puntos y con estructura diferente al anterior protocolo. "*IPV6 Aspectos Legales del nuevo protocolo de Internet". Euro6ix. Comisión Europea. http:// ipv6tf.org.*

[307] Los ordenadores se identifican por el número IP *(Internet Protocol)* establecido mundialmente y que queda registrado en todos los accesos a la red. Así en lo que concierne al correo electrónico la cabecera del mismo proporciona el número IP salvo en los casos de correo electrónico anónimo que ofrecen determinadas empresas o para los teléfonos móviles con sistema de prepago.

[308] STS 739/2008, de 12 de noviembre.

encuentran protegidos ni por el art. 18.1 CE, ni por el art. 18.3 CE (STS 1299/2011 de 17 de noviembre; STS 292/2008, de 28 de mayo; y STS 776/2008, de 18 de noviembre)[309], por lo que la Policía puede obtener la identificación IP sin que sea necesario obtener autorización judicial.

Ahora bien, es preciso tener en cuenta que la jurisprudencia distingue por un lado, los casos de rastreo policial del espacio público, y por otro los supuestos en los que para acceder a una información sobre IP es necesario oficiar a una operadora ISP[310].

Los rastreos policiales para localizar direcciones IP pueden realizarse sin necesidad de autorización judicial ya que no se trata de datos confidenciales preservados del conocimiento público. La barrera entre lo público (la Red), en donde la policía y cualquier particular pueden rastrear los vestigios dejados por el atacante informático, y lo privadamente protegido, donde no cabe inmiscuirse legalmente salvo que lo permita el afectado o lo autorice un juez, es la seña IP *(Internet Protocol* o número identificativo singularizado e irrepetible necesario para poder acceder a Internet), para el conocimiento de cuyos datos asociados debe existir autorización judicial[311].

De especial interés se muestra la STS 1299/2011 de 17 de noviembre[312] en la que se establece [FJ 5] que:

a) Los rastreos que realiza el equipo de delitos telemáticos de la Guardia Civil en Internet tienen por objeto desenmascarar la identidad críptica de los IPS (Internet Protocols) que habían accedido a los "hash" que contenían pornografía infantil. El acceso a dicha información, calificada de ilegítima o irregular, puede efectuarla cualquier usuario. No se precisa autorización judicial para conseguir lo que es público y

[309] Circular 1/2013 de la Fiscalía General del estado, sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas. Madrid 11 de enero de 2013.

[310] En este último supuesto, sí debe considerarse necesario obtener autorización judicial conforme a las previsiones del art. 588 ter k de la LECrim y de la Ley 25/2007, de conservación de datos (SSTS 292/2008, de 28 de mayo, 236/2008, de 9 de mayo, 680/2010, de 14 de julio). Aquí la exigencia deriva del mandato legal pese a que el dato no pueda cobijarse bajo el manto protector del secreto de las comunicaciones.

[311] Circular 1/2013 de la Fiscalía General del estado, sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas. Madrid 11 de enero de 2013.

[312] En idéntico sentido *vid*. las SSTS 680/2010, de 14 de julio, 739/2008, de 12 de noviembre, 236/2008, de 9 de mayo, y 292/2008, de 28 de mayo.

el propio usuario de la red es quien lo ha introducido en la misma. La huella de la entrada queda registrada siempre y ello lo sabe el interesado[313]. Consecuentemente -aclara la referida sentencia- quien utiliza un programa P2P ("peer-to-peer", de par a par o de igual a igual), como el EMULE, asume que muchos de los datos se convierten en públicos para los usuarios de internet, circunstancia que conocen o deben conocer los internautas, y tales datos conocidos por la policía, datos públicos en internet, no se hallan protegidos por el art. 18.1 ni por el art. 18.3 de la Constitución[314].

b) Se hace preciso acudir a la autorización del juez instructor para desvelar la identidad de la terminal, teléfono o titular del contrato de un determinado IP, en salvaguarda del derecho a la intimidad personal (habeas data)[315].

En definitiva, la jurisprudencia y ahora también la LECrim, distinguen entre la obtención por la Guardia Civil o Policía de la IP, que se puede hacer sin necesidad de pedir autorización judicial, y la identificación del titular del terminal, para lo cual sí es necesario, pues tras la averiguación del IP, las subsiguientes actuaciones de

[313] En el mismo sentido, prosigue la STS 680/2010, de 14 de julio, al tratar de los rastreos informáticos policiales, "*la STS 292/2008, de 28 de mayo, ya declaró que cuando la comunicación a través de la Red se establece mediante un programa P2P, como en el EMULE o EDONKEY, al que puede acceder cualquier usuario de aquella, el operador asume que muchos de los datos que incorpora a la Red pasen a ser de público conocimiento para cualquier usuario de internet, como, por ejemplo el IP, es decir, la huella de la entrada al programa, que queda registrada siempre. Y fue este dato, el IP del acusado, el que obtuvo la Guardia Civil en su rastreo de programas de contenido pedófilo, dato que -conviene repetir y subrayar- era público al haberlo introducido en la Red el propio usuario al utilizar el programa P2P. Por ello, no se precisa autorización judicial para conocer lo que es público, y esos datos legítimamente obtenidos por la Guardia Civil en cumplimiento de su obligación de persecución del delito y detención de los delincuentes, no se encontraban protegidos por el art. 18.3 CE.*"

[314] SAP Córdoba (Sección 3ª) 363/2014, de 18 julio (sobre rastreo policial de archivos informáticos).

[315] Y con el fin de aclarar todavía más una cuestión que siempre presenta un componente técnico de cierta complejidad, añade la referida STS 680/2010, remitiéndose a su vez a la 292/2008, de 28 de mayo que debe recordarse que el IP del acusado que averiguó la Guardia Civil no identifica la persona del usuario, para lo cual se precisa conocer el número del teléfono y la titularidad del contrato con la autorización judicial. Y si, como ha quedado razonado, la obtención por la Guardia Civil del IP del acusado -única actuación policial en todo el procedimiento de investigación no controlada y dirigida por la autoridad judicial-, no ha quebrantado el derecho constitucional al secreto de las comunicaciones proclamado en el art. 18.3 C.E, debemos ahora enfocar el problema desde la perspectiva de las disposiciones legales que tienen por finalidad desarrollar la protección de la intimidad de las personas que consagra el art. 18.1 C.E y, en concreto, la protección de datos personales que afecten a esa intimidad (art. 18.4 CE).

identificación y localización de quién sea la persona que tiene asignada dicha etiqueta numérica, se deben llevar a cabo bajo control judicial[316].

Así el artículo 588 ter k de la LECrim dispone que: *"Cuando en el ejercicio de las funciones de prevención y descubrimiento de los delitos cometidos en internet, los agentes de la Policía Judicial tuvieran acceso a una dirección IP que estuviera siendo utilizada para la comisión algún delito y no constara la identificación y localización del equipo o del dispositivo de conectividad correspondiente ni los datos de identificación personal del usuario, solicitarán del juez de instrucción que requiera de los agentes sujetos al deber de colaboración según el artículo 588 ter e, la cesión de los datos que permitan la identificación y localización del terminal o del dispositivo de conectividad y la identificación del sospechoso."*

En definitiva, una vez obtenida la IP, será necesaria autorización judicial para la cesión de datos que permitan identificar y localizar el dispositivo o terminal, así como los datos de identificación personal del usuario.

Por último, hay que tener presente que según la STS 8316/2012, de 3 de diciembre, el hecho de que una persona sea titular de una línea con una concreta dirección IP desde la que se ha cometido un delito, no es cuestión necesaria y suficiente para culpabilizar al titular de la línea de la comisión del delito si no existen otras pruebas.

2.2 Identificación de IMEI, IMSI y MAC.

Con el término IMSI se hace referencia a un código de identificación único para cada línea de telefonía móvil integrada en la tarjeta SIM (*Subscriber Identy Module*) que permite la identificación del abonado a través de las redes GSM y UMTS.

[316] En este sentido la STS 739/2008, de 12 de noviembre indica que "averiguado el lP de quien obtenía el material pedófilo, mediante el rastreo policial del espacio público, las subsiguientes actuaciones de identificación y localización de quien tenía asignado ese IP se llevaron a cabo bajo control judicial".

Por su parte, el término IMEI es un código pregrabado en los teléfonos móviles que identifica al aparato unívocamente a nivel mundial y se trasmite por el móvil a la red de telefonía al conectarse a ésta. Es el equivalente al número mac, cuando nos referimos a móviles, pues identifica ese número de serie al equipo.

El término MAC es un identificador de 48 bits que corresponde de forma única a una tarjeta o dispositivo de red, también conocida como dirección física y es única para cada dispositivo. Las direcciones Mac son únicas a nivel mundial y constituyen una huella digital que permite determinar desde qué dispositivo de red se ha emitido un determinado paquete de datos.

Tanto el MAC, el IMEI y el IMSI carecen de capacidad de información sobre la identidad del usuario, teniendo valor únicamente si se asocia a otros datos en poder de las operadoras. La captación de tales números a efectos de investigación penal es posible mediante un escaneado o barrido realizado a través de instrumentos electrónicos que detectan aquellos siempre que se actúe en un determinado radio de acción en el que se encuentra el terminal. Su captación se realiza como consecuencia de un seguimiento dirigido específicamente frente a un individuo o individuos determinados[317].

Con posterioridad a la captación, una vez obtenido el correspondiente código identificativo, es necesaria la obtención del número comercial del teléfono, en posesión de la prestadora del servicio de telecomunicación. Ni el MAC, ni el IMSI, ni el IMEI por sí solos, son datos integrables en el concepto de comunicación.

En cuanto a la obtención de los IMSI, el TS refrenda la legitimidad de que sea la propia policía quien los obtenga por sus medios técnicos en la medida que con ellos se desconoce incluso el número telefónico concernido y las llamadas que pudieran recibirse y efectuarse (STS 1115/2011, de 17 de noviembre; STS 79/2011, de 15 de febrero; STS 249/2008, de 20 de mayo; STS 776/2008, de 18 de noviembre).

[317] Es posible obtener el *IMSI* de un teléfono móvil mediante un aparato especial que simula el comportamiento de la red GSM y con el que inicia un diálogo de forma equivalente al que se sigue en la infraestructura de red de un operador móvil cuando se enciende el móvil o se cambia de célula de cobertura. Para ello es preciso que el aparato se utilice en las proximidades del teléfono que se desea investigar.

La utilización de herramientas electrónicas que rastrean el espectro radioeléctrico forzando a los dispositivos cercanos a generar un diálogo automático con la herramienta a través de la que facilitan a ésta las asignaciones numéricas que se corresponden con los números IMEI o IMSI se encontraba carente de una cobertura legal; más allá de una consolidada jurisprudencia del Tribunal Supremo que sistemáticamente validaba tal forma de investigación, siempre que a través de este vía no se accediera a lo que eran auténticos datos de tráfico de comunicaciones[318]

La LECrim, de acuerdo con la jurisprudencia, regula la identificación de los terminales mediante captación de códigos de identificación como el IMSI o el IMEI, habilitando a los Cuerpos Policiales a la utilización de artificios técnicos que permitan su obtención, sin necesidad de autorización judicial (artículo 588 ter l LECrim).

Aunque la LECrim no hace referencia expresa al término MAC, como sucede con el IMSI e IMEI debería entenderse incluido también en la fórmula abierta y amplia utilizada en este precepto. Ahora bien, tanto con el IMSI como con el IMEI o MAC se dispone de información suficiente como para poder solicitar la identificación por el operador de los números de teléfono que corresponden a tales datos, o la correspondiente intervención de las comunicaciones. Pero no puede la Policía solicitar directamente tal información de las operadoras. La Ley 25/2007, de 18 de octubre, *de Conservación de Datos de las Comunicaciones Electrónicas*, incluye en el art. 3.1 dentro de su ámbito de aplicación los datos IMSI, IMEI y MAC para cuya cesión resulta exigible la misma regla impuesta para el resto de los datos a los que se refiere, esto es,

[318] STS 249/2008, de 20 de mayo, que establecía que "*está fuera de dudas que el IMSI, por sí solo, no es susceptible de ser incluido en alguna de esas dos categorías. Ni es un dato integrable en el concepto de comunicación, ni puede ser encuadrado entre los datos especialmente protegidos. Ese número de identificación sólo expresa una serie alfanumérica incapaz de identificar, por su simple lectura, el número comercial del abonado u otros datos de interés para la identificación de la llamada. Para que la numeración IMSI brinde a los investigadores toda la información que alberga, es preciso que esa serie numérica se ponga en relación con otros datos que obran en poder del operador. Y es entonces cuando las garantías propias del derecho a la autodeterminación informativa o, lo que es lo mismo, del derecho a controlar la información que sobre cada uno de nosotros obra en poder de terceros, adquieren pleno significado. Los mismos agentes de Policía que hayan logrado la captación del IMSI en el marco de la investigación criminal, habrán de solicitar autorización judicial para que la operadora correspondiente ceda en su favor otros datos que, debidamente tratados, permitirán obtener información singularmente valiosa para la investigación. En definitiva, así como la recogida o captación técnica del IMSI no necesita autorización judicial, sin embargo, la obtención de su plena funcionalidad, mediante la cesión de los datos que obran en los ficheros de la operadora, sí impondrá el control jurisdiccional de su procedencia"*

la preceptiva autorización judicial[319]. Es precisa, pues, autorización judicial para la cesión de los datos IMSI y del IMEI por las operadoras, no porque se integren dentro del arco protector del secreto de las comunicaciones sino porque la Ley 25/2007, de 18 de octubre, y el artículo 588 ter l, apartado 2º de la LECrim, así lo exigen.

Es éste el sentido que ha de darse a la norma: una habilitación legal para, mediante herramientas tecnológicas -IMSI *cátcher-,* o incluso software diseñado precisamente para tal menester (por ejemplo, la emisión de mensajes que generen una respuesta automática del terminal investigado referentes a la identificación del mismo, como una confirmación de recepción que permita su geolocalización) adentrarse en esos componentes que permita la individualización del dispositivo o tarjeta a través del cual canalizar una injerencia sobre comunicaciones[320].

Se trataría de un auténtico acto previo a una solicitud de intervención de comunicaciones, aunque la posibilidad de utilización de tal estrategia, quedaría limitada a aquellos supuestos en los que pudiera ser procedente, en términos de tipos penales susceptibles de permitir en abstracto una injerencia. La norma, sin embargo, se muestra más ambiciosa y abre las puertas a otras posibilidades de indagación, de acuerdo con el estado de la tecnología[321]. La barrera infranqueable para estas vías de prospección se debe establecer en la prohibición de que el acceso a la información tenga lugar mediante cualquier forma o vía de interceptación que la extraiga de comunicaciones en curso, sometidos a la inexcusable previa autorización judicial de interceptación; o datos relativos a comunicaciones ya consumados, sometidos a la disciplina del art. 588 bis c.

[319] Circular 1/2013 de la Fiscalía General del estado, sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas. Madrid 11 de enero de 2013.

[320] RODRÍGUEZ LAINZ, J. L. "La interceptación de las comunicaciones telefónicas y telemáticas en el Anteproyecto (…)". ob. cit, pág. 17.

[321] Es decir, no solamente no se necesita autorización judicial para obtener el IMSI o IMEI, sino, en general, de cualquier medio técnico que, de acuerdo con el estado de la tecnología, sea apto para identificar el equipo de comunicación utilizado o la tarjeta utilizada para acceder a la red de telecomunicaciones. Así la STS 551/2016, de 22 de junio [FJ 2º] incluye también la obtención del número PIN del sistema operativo Os Blackberry pues entiende que "*el número de PIN es un dato de acceso a la terminal telefónica, cuyo conocimiento no requiere autorización judicial, por no tratarse de dato alguno relativo a las comunicaciones. En cierta manera, aunque no sea exactamente lo mismo, se parece a la obtención de los números correspondientes al chasis del terminal (IMEI), o al número internacional de la tarjeta telefónica (IMSI).*

La única puesta en conocimiento que se prevé de haberse realizado este tipo de prácticas, lo será en aquellos casos en los que, dando un resultado positivo, se interese de la autoridad judicial competente la intervención de las comunicaciones. Se deberá informar expresamente del origen de tal fuente de conocimiento, puesto que la solicitud habrá de poder comunicar al órgano jurisdiccional la utilización de los artificios para la captación de estos códigos (art. 588 ter l, apartado 2º, in fine).

Por ello, deberían arbitrarse mecanismos de puesta en conocimiento del empleo de tales herramientas, que permitieran su sometimiento a un mínimo control, bien por la autoridad judicial, bien por el Ministerio Fiscal[322].

2.3 Obtención de datos desvinculados de los procesos de comunicación.

2.3.A) Identificación de titulares o terminales o dispositivos de conectividad.

El artículo 41.1 de la Ley General de Telecomunicaciones establece la obligación de los operadores de garantizar los niveles de protección de datos exigidos por la LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).

En igual sentido, el artículo 48 de la citada Ley de Telecomunicaciones relaciona los derechos de privacidad de los abonados, y concretamente en su apartado 3 se refiere a la protección de datos y a la privacidad en relación con las guías de abonados.

De conformidad con lo dispuesto en el artículo 11 de la LOPD los datos de carácter personal solo podrán ser comunicados a terceros previo consentimiento del interesado, si bien no es preciso dicho consentimiento en los supuestos exceptuados en el mismo artículo, uno de los cuales es el siguiente:

[322] RODRÍGUEZ LAINZ, J. L. "La interceptación de las comunicaciones telefónicas y telemáticas en el Anteproyecto (…)". ob. cit. pág. 17.

Art. 11.2 f) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces y Tribunales o el Tribunal de Cuentas en el ejercicio de las funciones que tiene atribuidas.

Por tanto, la autoridad judicial puede acceder a la información sobre abonados, en todo caso, en el curso de una investigación criminal de acuerdo con el artículo 18 CE y con la normativa específica antes mencionada.

El Ministerio Fiscal podrá hacerlo inicialmente con base a lo dispuesto en el artículo 11.2 f) de la LOPD, antes citado, salvo que dicha información se encuentre vinculada al secreto de las comunicaciones o cuando se necesite dicha autorización judicial[323].

En lo que concierne a las Fuerzas y Cuerpos de Seguridad, en España tanto el Tribunal Constitucional como el Tribunal Supremo tradicionalmente han entendido que cuando el acceso a esa información no afecte al secreto de las comunicaciones, sino únicamente al derecho a la intimidad personal, y concurran circunstancias de urgencia y necesidad sería posible el acceso a dicha información en el ejercicio de sus funciones legitimas de prevención e investigación del delito, descubrimiento de los delincuentes y recogida de los instrumentos, efectos y pruebas del mismo[324].

No obstante, como se verá en los apartados correspondientes a la conservación y cesión de los datos de tráfico, en esta materia tuvo una gran incidencia la Ley 25/2007, de 18 de octubre, sobre conservación de datos de las comunicaciones electrónicas, que obliga a los operadores que presten tales servicios a conservar determinados datos (entre ellos datos de abonados) generados y tratados en el marco de la prestación de ese servicio y concretamente los previstos en el artículo 3 de dicha ley, necesarios para:

a) rastrear e identificar el origen de una comunicación.

---

[323] En este sentido, la STS 986/2006, de 19 de junio, declara expresamente [FJ 2º] que "*el art.11.2 de la LO 15/1999, de Protección de datos de carácter personal, exime de la exigencia del previo consentimiento del interesado los casos en que la comunicación de datos tenga por destinatario al Ministerio Fiscal, en el ejercicio de las funciones que éste tiene atribuidas"*.

[324] Con apoyo en artículos 282 de la Ley de Enjuiciamiento Criminal, el artículo 11.1 de la LO 2/1986 de 13 de marzo de Fuerzas y Cuerpos de Seguridad y el artículo14 de la derogada LO 1/1992 de 21 de febrero sobre Protección de la Seguridad Ciudadana.

b) Identificar el destino de una comunicación.

c) Determinar la fecha, hora y duración de una comunicación.

d) Identificar el tipo de comunicación.

e) Identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación.

En relación con los datos referidos a abonados que se recogen en el citado artículo 3, la Ley 25/2007, en su artículo 1 fija un régimen especial a cuyo tenor estos solo pueden ser entregados por los operadores a requerimiento de la autoridad judicial.

Si el acceso a los datos de tráfico conservados por una operadora de comunicaciones al amparo de lo dispuesto en la ley 25/2007 precisa autorización judicial. La reclamación a las operadoras de la identificación del titular a partir de los datos de un dispositivo, o determinar los dispositivos de los que es titular una persona concreta, realizada por la Policía Judicial o el Ministerio Fiscal en el curso de una investigación concreta no lo precisa; tal y como establece el art. 588 ter m[325].

Sería conveniente que la policía expresara el modo por el que llega a su conocimiento la identificación del titular, de los terminales o dispositivos de conectividad, a los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, a quien se lo hayan solicitado, aunque la ausencia de estos datos no invalida lo obtenido[326].

[325] Se respeta el principio de proporcionalidad de la medida, ya que el derecho a la intimidad del interesado se vería muy débilmente afectado y primaría el interés público en la investigación y esclarecimiento de un hecho delictivo.

[326] La STS 309/2010, de 31 de marzo establece que "*la representación legal del acusado reivindica la nulidad de esas escuchas con el argumento añadido de que no consta cómo los agentes pudieron obtener conocimiento de tres de los números que fueron objeto de interceptación. Si bien se mira, el argumento encierra un salto dialéctico que quiebra su razonabilidad. Como en el oficio inicial no se dijo nada acerca de la forma de obtención de esos números de teléfonos, habremos de concluir que la policía sólo pudo obtenerlos mediante técnicas de escaneo proscritas y, por tanto, con vulneración del derecho a la inviolabilidad de las comunicaciones. Sin embargo, tal línea de razonamiento no puede ser aceptada por la Sala. Los números de teléfono usados por los imputados pueden ser obtenidos de muy distintas fuentes. Y no necesariamente ilícitas. Esta Sala ha señalado, es cierto, que cuando se acredita la injerencia de los poderes públicos en el ámbito protegido por un derecho fundamental, aquellos deben estar en condiciones de acreditar la legitimidad de su actuación, pues la regla general es la vigencia del derecho, y constituyendo su restricción una excepción, ésta debe estar debidamente justificada (cfr. STS 130/2007,*

2.3.B) Acceso a datos no integrados en un proceso de comunicación (agenda de un teléfono móvil).

Más dudoso era el supuesto de si el Fiscal y la policía podían acordar el acceso a documentos no integrados en un proceso de comunicación y archivados en teléfonos móviles, ordenadores o asimilados, cuando concurrían razones de urgencia[327].

Como ya se ha señalado, excepcionalmente se ha legitimado a la Policía para que con la suficiente y precisa habilitación legal realice determinadas prácticas que constituyen una injerencia leve en la intimidad de las personas, siempre que se hayan respetado las exigencias dimanantes del principio de proporcionalidad (STC 142/2012, de 2 de julio y STC 281/2006, de 9 de octubre)[328].

La apertura de una agenda y la lectura de lo encontrado en ella incide en el derecho a la intimidad (STC 70/2002, de 3 de abril), pero no en el secreto de las comunicaciones. Igualmente, se había puesto de manifiesto que, a pesar de las múltiples funciones de un ordenador personal, el acceso a su contenido podrá afectar bien al derecho a la intimidad personal (art. 18.1 CE), bien al derecho al secreto de las

---

19 de febrero). Sin embargo, en el caso que nos ocupa, no existe ningún indicio que permita afirmar razonadamente que tal injerencia se haya producido, habida cuenta que, pudiendo haberse obtenido el número de teléfono del sospechoso por múltiples vías legítimas, nada indica que la utilizada no lo haya sido. Y así como no es posible presumir la legalidad de la injerencia, obligando al afectado a demostrar que su derecho ha sido restringido indebidamente, tampoco es posible presumir la misma existencia de dicha injerencia, si caben otras opciones respetuosas con la Constitución y la ley, como pueden ser las noticias recibidas de confidentes, agentes infiltrados, colaboradores, u otras intervenciones telefónicas. Dicho de otra forma, es exigible a los poderes públicos que justifiquen que la restricción de un derecho fundamental se ha realizado con respeto a las reglas, pero no lo es que demuestren que no lo han hecho (cfr. STS 509/2009, 13 de mayo)". (En el mismo sentido, la STS 246/2014, de 2 de abril).

[327] La STS 782/2007, de 3 de octubre [FJ 2] (policía visiona, sin autorización judicial, las imágenes grabadas por un particular) y la STC 173/2011, de 7 de noviembre (sobre acceso por la policía a imágenes de un ordenador). La habilitación a la policía se hace extensida al M. Fiscal.

[328] *"La visión del número emisor que automaticamente aparece en la pantalla del receptor al margen de la voluntad de quien llama, y perceptible por cualquiera que tenga a la vista el aparato no entraña interferencia en el ámbito privado de la comunicación; ni tampoco lo es la previa comprobación de la memoria del aparato, que tiene a tal efecto el simple carácter de una agenda electrónica y no la consideración de un teléfono en funciones de transmisión del pensamiento dentro de una relación privada de comunicación entre dos personas"* (SSTS 1273/2009, de 17 de diciembre [FJ 2], 1397/2005, de 30 de noviembre [FJ 1]. "La utilización de los contenidos de los teléfonos para obtener los números de algunas personas no implica ilicitud porque la simple averiguación de los números telefónicos de contacto no constituye propiamente una injerencia en el secreto de las comunicaciones" (STS 112/2007, de 16 febrero).

comunicaciones (art. 18.3 CE) en función de si lo que resulta desvelado a terceros son, respectivamente, datos personales o datos relativos a la comunicación (SSTC 142/2012, de 2 de julio; 173/2011, de 7 de noviembre y STS 663/2011, de 7 de julio).

A tales efectos se distinguía entre el acceso a la libreta de direcciones y el acceso al registro de llamadas[329]. En este sentido, cuando el acceso de la Policía al teléfono móvil del investigado se limita a los datos recogidos en el archivo de contactos telefónicos pero no al registro de llamadas efectuadas y/o recibidas, debía concluirse que dichos datos no forman parte de una comunicación actual o consumada, ni proporcionan información sobre actos concretos de comunicación pretéritos o futuros. Con el acceso a la agenda de contactos telefónicos no se obtiene información concerniente a la transmisión de comunicación emitida o recibida por el celular, sino únicamente un listado de números telefónicos introducidos voluntariamente por el usuario del terminal sobre los que no consta si han llegados a ser marcados[330]

Una primera doctrina consideraba que lo decisivo para la delimitación del contenido de los derechos fundamentales recogidos en los arts. 18.1 y 18.3 CE no era el tipo de soporte, físico o electrónico, en el que la agenda de contactos se encontrara ni el hecho de que la agenda fuese una aplicación de un terminal telefónico móvil, sino el carácter de la información a la que se accede (STC 142/2012, de 2 de julio).

---

[329] La STC 115/2013, de 9 de mayo, claramente distingue entre el acceso a la agenda de un móvil, que no precisa autorización judicial, y el acceso al listado de llamadas, que sí lo precisaría.

[330] VÁZQUEZ SECO, L. "Incorporación de datos al proceso. Vigencia de la Ley 25/2007 de 18 de octubre de conservación de datos relativos a las comunicaciones electrónicas y redes públicas e interpretación de la Ley a la luz de la reforma operada por LO 13/2015". Ponencia presentada en el curso de Formación de Fiscales "Uso de las nuevas tecnologías y nuevas formas de delincuencia" que se celebró en el Centro de Estudios Jurídicos los días 27 al 28 de octubre de 2016, págs. 16 y 17 "*Habrá que esperar que la jurisprudencia clarifique ciertos supuestos controvertidos, como son los datos de posicionamiento que emiten por ejemplo los terminales móviles al margen de una comunicación concreta (un teléfono móvil encendido, aunque no se utilice para ninguna comunicación, al desplazarse el usuario el terminal va saltando de una celda a otra en busca de señal según la antena de comunicación más próxima con la que se conecte, y esa información puede ser recuperada, y la cuestión está en que esos datos de localización se generan al margen de una comunicación concreta; parece claro que esa información permite seguir los movimientos de su titular, por lo que afecta al derecho a la intimidad y por tanto de la cobertura de una autorización judicial; o supuestos que sin duda se generaran en el futuro con la expansión de la denominada " internet de las cosas" donde la comunicación no es entre personas sino entre máquinas, aunque utilizando el mismo razonamiento esos aparatos electrónicos se comunican previa programación de una persona, y esa programación junto a las comunicaciones realizadas en ejecución de la misma parece claro que también están bajo el ámbito reservado protegido por el derecho a la intimidad)".*

Hoy día esta distinción se entiende superada por la generación del nuevo *derecho a la identidad virtual* y por aplicación del artículo 588 sexies c apartados 3º y 4º, que permite a la policía, en caso de urgencia, acceder al contenido de los dispositivos sea cual sea el mismo, sin especificar si se accede a datos vinculados o no a procesos de comunicación y siempre que se informe al juez competente dentro del plazo máximo de veinticuatro horas. Pero esta posibilidad de que acceda la policía a una agenda de teléfono móvil, sin autorización judicial, se limita exclusivamente a los supuestos de urgencia, que se detallarán más adelante.

2.4 La Orden de Conservación de Datos.

2.4.A) Concepto de Datos Informáticos.

A la hora de analizar y de investigar estos ilícitos, es importante emplear con precisión una serie de conceptos asociados al uso de las nuevas tecnologías, y saber diferenciar los diferentes datos informáticos que serán relevantes en el transcurso del proceso. Por datos informáticos debemos entender, siguiendo la terminología del Convenio del Consejo de Europa sobre Ciberdelincuencia, en su artículo 1.B: "*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"*.

Del conjunto de los datos informáticos hay que diferenciar los "**datos de contenido"** y los "**datos de tráfico**". Los datos de contenido constituyen la información que se comunica o trasmite, mientras que los datos de tráfico[331], son "*todos los datos relativos a una comunicación realizada por medio de un sistema informático,*

[331] En el derecho interno, el RD 424/2005 de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, define los datos de tráfico en su artículo 64.a) como *cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de su facturación.*
El mismo artículo en su apartado c) define *comunicación como cualquier información intercambiada o conducida entre un numero finito de interesados por medio de un servicio de comunicaciones electrónicas disponible para el público.*

generados por éste último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación, o el tipo de servicio subyacente, (artículo 1.d del Convenio sobre ciberdelincuencia).

En consecuencia, los datos de tráfico incluyen:

a) los referidos al IP (Internet Protocol que identifica el equipo o terminal informática) del equipo emisor.
b) Los relativos a los sistemas o equipos de tránsito[332], servidores de la red o proveedores de acceso o de servicios, y
c) los referidos al equipo o sistema destinatario final.

Así, el término "origen", viene referido tanto al número de teléfono, como la dirección IP o similar identificación de una terminal de comunicaciones a la que un proveedor de servicios ha prestado servicios. Asimismo el término "destino" viene referido a una indicación similar de una terminal informática o de comunicaciones a la que ha sido transmitida la comunicación. Y el término "tipo de servicio subyacente" viene referido al tipo de servicio que ha sido usado a través de la red (transferencia de archivos, correo electrónico o mensaje instantáneo, entre otros)[333].

Junto a los tipos anteriores hay que señalar también a los "**datos relativos a los abonados"**, que el art. 18.3 del CSC conceptúa "*como cualquier información, en forma de datos informáticos o de cualquier otro modo que posea un proveedor de servicios, y que se refiera a los abonados de sus servicios, diferentes de los datos relativos al tráfico o al contenido, y que permitan determinar:*

a) el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el período de servicio;

b) la identidad, dirección postal o situación geográfica y número de teléfono del abonado, así como cualquier otro número de acceso, y los datos relativos a la

[332] En los pasos de la comunicación por internet la identificación del servidor queda registrada en los .log o registro de sucesos de los ordenadores, de los que se puede obtener, por tanto, datos de sumo interés.

[333] ROVIRA DEL CANTO, E. "Las nuevas pruebas telemática y digitales (…)". ob. cit. pág. 27.

facturación y al pago, disponibles en virtud de un contrato o de un acuerdo de prestación de servicio;

c) cualquier otra información relativa al lugar en que se encuentren los equipos de comunicación, disponibles en virtud de un contrato o de un acuerdo de prestación de servicio.

Asimismo, la Consulta 1/1999 de la Fiscalía General del Estado distingue como un tercer orden distinto a los datos de contenido y a los de tráfico los que denomina "datos de los abonados" (necesarios para la prestación del servicio pero no generados en el proceso de comunicación). En tal sentido, el término "disposiciones técnicas" que recoge el Convenio viene referido a todas las medidas que facilitan al suscriptor el disfrute del servicio ofrecido, y que incluirán de ordinario un número técnico o dirección (número de teléfono, dirección web o nombre de dominio, dirección de correo electrónico), así como la identificación del equipo de comunicaciones usado por el suscriptor (aparato de teléfono, centros de llamada o LANs (redes de área local).

Es precisamente en el ámbito de la conexión donde los tipos "datos de tráfico" y "datos del suscriptor o abonado" convergen, dando lugar a lo que diversos autores denominan "datos de conexión", si bien podemos incluirlos en términos generales dentro del segundo tipo[334]. Ciertamente como sostiene la Fiscalía General el Estado en la precitada Consulta, los datos de contenido tienen su protección reconocida a nivel constitucional en el art. 18.3 de la CE (secreto de las comunicaciones), y los relativos a los datos de abonado en la protección al derecho a la intimidad personal conforme al art. 18.4 CE.

La LECrim incorpora en el artículo 588 ter b) un concepto de datos electrónicos de tráfico o asociados en los siguientes términos: "*A los efectos previstos en este artículo se entenderá por datos electrónicos de tráfico o asociados, todos aquellos que se generan como consecuencia de la conducción de la comunicación a través de una red de comunicaciones electrónicas, de su puesta a disposición del usuario, así como de la prestación de un servicio de la sociedad de la información o comunicación telemática de naturaleza análoga".*

[334] ROVIRA DEL CANTO, E. "Las nuevas pruebas telemática y digitales (…)". ob. cit. pág. 28.

Es indispensable contar con la cooperación de los operadores de telecomunicaciones y los proveedores de servicios de internet, al ser éstos quienes poseen la información necesaria sobre los abonados y suscriptores así como el tráfico de comunicaciones anteriores generados por el equipo, con registro de detalles tales como la hora, la duración y la fecha de cualquier comunicación, las partes que la sostuvieron o el tipo de servicio o actividad. Estos datos se conservan por lo general durante un período limitado, según las necesidades comerciales del operador o proveedor y los requisitos legales o comerciales para la protección de la esfera privada.

2.4.B) Régimen jurídico de la Órden de Conservación de Datos.

El artículo 16 del CSC establece la inmediata conservación de datos informáticos específicos, incluyendo datos de tráfico que hayan sido almacenados por medio de un sistema informático cuando haya serios indicios de que los datos puedan perderse o ser modificados. Obliga a la conservación de la integridad de dichos datos por un período de tiempo necesario, hasta un máximo de 90 días, a fin de facilitar a las autoridades competentes su revelación, con posibilidad de renovación del período de vigencia de la orden.

Asimismo el CSC prevé que se pueda obligar al custodio o al tercero que conserve los datos informáticos a que mantengan secreto tanto sobre la propia orden como de la práctica de la medida, y por el período de tiempo que se establezca en la normativa interna[335].

[335] ROVIRA DEL CANTO, E. "Las nuevas pruebas telemática y digitales (…)". ob. cit. pág. 48. "*Este procedimiento es novedoso y su utilidad es evidente en la lucha contra la criminalidad informática, sobre todo en relación con las infracciones cometidas a través de internet. En primer lugar, porque los datos informáticos como hemos indicado, por su alta volatilidad, son fáciles de manipular y modificar. Es fácil perder datos susceptibles de probar la infracción si el almacenamiento no se lleva cabo correctamente, si los datos son manipulados o alterados intencionalmente para destruir la fuente de prueba o si su destrucción tiene lugar en el marco o de operaciones normales de borrado de datos considerados inútiles. Uno de los métodos clásicos para preservar la integridad de los datos sería mediante la ya analizada tradicional entrada y registro de locales y en el sistema informático del poseedor de los datos. Ahora bien, aparte de los inconvenientes que ya hemos expuesto con anterioridad respecto de tal medida, en pro de la presente se argumenta que cuando el custodio de los datos es digno de confianza, como sería el caso de una empresa de fama acreditada (e interesada por tanto en mantenerla), la conservación*

Esta medida, como la prevista en el artículo siguiente, se aplica exclusivamente a aquellos datos preexistentes que han sido ya recogidos y almacenados por un poseedor en su sistema informático, (por ejemplo, por un proveedor de servicios de acceso a internet a los efectos de facturación). No se aplica para la obtención e interceptación en tiempo real de futuros datos de tráfico ni tampoco al acceso en tiempo real al contenido de comunicaciones, pues estas medidas son ya las específicas de los arts. 20 y 21[336].

En realidad, el art. 16 como el 17 del CSC, facultan a las autoridades encargadas de perseguir los ciberdelitos a requerir, en el marco de un procedimiento penal específico ya abierto, la conservación de aquellos datos que se encuentren previamente archivados o almacenados y que pudieran ser necesarios para la identificación de los autores o como fuente de prueba[337].

---

adecuada de los datos puede quedar mejor garantizada mediante la presente orden de conservación dirigida a la empresa en cuestión. Y una orden de conservación siempre resultará menos lesiva para el funcionamiento y la reputación de la empresa en cuestión que una operación de entrada y registro policial. Además, hay que recordar que los delitos informáticos se cometen, a menudo, mediante la transmisión de comunicaciones (material pornográfico, virus, datos falsificados) a través de las redes informáticas. La identificación de la fuente o del destino final de tales comunicaciones puede permitir la identificación del autor o autores. Finalmente, la conservación de datos (por ejemplo, correos electrónicos) puede permitir probar la actuación criminal independientemente de que se trate de delitos cibernéticos específicos o comunes realizados a través de Internet u otra red telemática".

[336] Convenio del Consejo de Europa relativo a la protección de la persona en relación con el tratamiento automatizado de datos de carácter personal, STE núm. 108, Selección de Tratados del Consejo de Europa. Les éditions du Conseil de l'Europe, F-67075. Strasbourg. Cedex. Directivas 95146IEC y 97/66IEC sobre protección de datos. Durante la negociación del Convenio fue este uno de los aspectos clave que más debate suscitó. *En algunos borradores o versiones se contempló la posibilidad de imponer a los proveedores de servicios la obligación de almacenar o recoger con carácter general ciertos datos que pudieran ser necesarios ulteriormente a los efectos de una investigación penal. Sin embargo, los proveedores de servicios y la industria informática objetaron los costos excesivos que tal obligación implicaría y rehusaron participar en el control de la ciberdelincuencia, labor ésta que estimaron que no debe recaer en las empresas privadas. Asimismo desde otros ámbitos se sostuvo que una obligación general de archivar datos podría ser contraria al derecho, al respeto a la intimidad y al secreto de la telecomunicaciones, garantizadas por el art. 8 del Convenio Europeo de Derechos Humanos, e infringir también la legislación europea en materia de protección de datos Por ello, el Convenio se refiere a 1a conservación de datos y no incluye obligación alguna de archivar, almacenar o coleccionar datos de un tipo u otro.*

[337] ROVIRA DEL CANTO, E. "Las nuevas pruebas telemática y digitales (…) ob. cit. pág. 47. Sostiene que hay que diferenciar entre las expresiones "conservación de datos" (en la versión original inglesa "*data preservation"*) y "archivo de datos" ("*data retention")* que tienen un contenido jurídico claramente diferenciado. Conservar implica guardar o custodiar datos previamente almacenados o archivados, protegiéndolos contra cualquier riesgo o amenaza que pudiera alterar o degradar su calidad o estado presente. Mientras que archivar quiere decir guardar en posesión de uno para un uso futuro aquellos datos que están siendo producidos en el momento presente. El archivo equivale al almacenamiento o la colecta de datos, mientras que la conservación es la actividad consistente en garantizar su seguridad y su integridad.

Esta orden de conservación de datos, no debe confundirse con la obligación genérica que tienen la operadoras de conservar o retener los datos[338].

En España, la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, abordó por primera vez el tema de la obligación de las operadoras de retener datos de tráfico relativos a las comunicaciones electrónicas en su artículo 12, si bien lo hizo de una forma vaga e imprecisa remitiéndose en cuanto a los detalles a una normativa de desarrollo que no vio la luz hasta la Ley 25/2007, de 18 de octubre, *de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones,* donde se reguló por primera vez esta materia[339].

La Ley es respetuosa con los pronunciamientos que, en relación con el derecho al secreto de las comunicaciones, ha emitido el Tribunal Constitucional, respeto que, especialmente, se articula a través de dos garantías: a) que los datos sobre los que se establece la obligación de conservación son datos exclusivamente vinculados a la comunicación, ya sea telefónica o efectuada a través de internet, pero en ningún caso reveladores del contenido de ésta; y, b) que la cesión de datos que afecten a una comunicación o comunicaciones concretas, exigirá siempre, la autorización judicial previa.

La Ley 25/2007 establece de manera precisa y detallada el listado de datos que quedan sujetos a la obligación de conservación en el marco de las comunicaciones por telefonía fija, móvil o internet (art.3). Todos estos datos deberán conservarse doce meses, contados desde la fecha en la que se produjo la comunicación, no pudiéndose conservar ningún otro que pudiera revelar el contenido de la misma (art. 5 de la Ley

[338] TEJADA DE LA FUENTE, E. "La retención obligatoria de los datos de tráfico (…)". ob. cit. pág. 319 distingue entre la retención obligatoria por disposición legal de los datos de tráfico y la preservación, en investigaciónes específicas de todo tipo de datos a efectos de su incorporación al proceso.

[339] Dictada en transposición de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modificó la Directiva 2002/58/CE. A pesar de la anulación por parte del Tribunal de Justicia de la Unión Europea de la Directiva 2006/24/CE, la Ley 27/2007 sigue plenamente vigente (sólo se podría dejar sin efecto mediante su derogación por el legislativo o por su anulación por el Tribunal Constitucional al resolver un recurso de inconstitucionalidad contra ella por la vulneración de los derechos fundamentales a la intimidad y a la protección de datos - artículos 18.1 y 18.4 de la Constitución Española- recurso que por el momento no ha sido interpuesto, o bien se someta al Tribunal de Justicia de la Unión Europea para que dictamine si la actual regulación es acorde o no con el derecho de la Unión mediante el planteamiento de la correspondiente cuestión prejudicial por los tribunales internos, esta eventualidad sí se ha producido como veremos en otro apartado de este escrito).

25/2007). De este modo, los operadores tienen la obligación genérica de conservar datos de tráfico y cederlos a la policía o el Ministerio Fiscal cuando lo soliciten con autorización judicial.

Como consecuencia lógica para dar efectividad a la obligación de conservación de datos y su eventual utilización posterior está la previsión de que el interesado no tiene derecho a la cancelación de los datos que se conserven ni tampoco tendrá que ser informado de su cesión.

Sin embargo, la orden de conservación de datos prevista en el 588 octies de la LECrim se regula como medida de aseguramiento y supone la incorporación definitiva al ordenamiento interno del art. 16 del Convenio sobre Ciberdelincuencia[340]. Se trata de una medida específica vinculada con las investigaciones concretas.

La finalidad de esta medida es garantizar la preservación de los datos e informaciones concretas de toda clase (no solo los datos de tráfico) que se encuentren almacenados en un sistema informático hasta que se obtenga la autorización judicial correspondiente para su cesión. De este modo, su posterior aportación como medio de prueba o, en su caso, su análisis forense no se verá frustrado por la desaparición, alteración o deterioro de unos elementos inherentemente volátiles. Se establece un plazo máximo de vigencia de la orden de noventa días prorrogable hasta que se autorice la cesión o se cumplan ciento ochenta días.

---

[340] Esta medida, en definitiva, no sólo resulta de gran importancia para la eficacia de las investigaciones nacionales relacionadas con los ciberdelitos sino también para dar cumplimiento a los compromisos internacionales asumidos por España, y concretamente a los que se derivan de la ratificación de la Convención de Budapest. Artículo 16 del Convenio sobre Ciberdelincuencia - Conservación inmediata de datos informáticos almacenados.
"1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para permitir a sus autoridades competentes ordenar o imponer de otro modo la conservación inmediata de datos electrónicos especificados, incluidos los datos de tráfico, almacenados a través de un sistema informático, especialmente cuando hayan razones para pensar que son particularmente susceptibles de pérdida o de modificación.
2. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar a una persona a conservar y proteger la integridad de los datos – que se encuentran en su poder o bajo su control y respecto de los cuales exista un mandato previo de conservación en aplicación del párrafo precedente – durante el tiempo necesario, hasta un máximo de 90 días, para permitir a las autoridades competentes obtener su comunicación. Los Estados podrán prever que dicho mandato sea renovado posteriormente.
3. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar al responsable de los datos o a otra persona encargada de conservarlos a mantener en secreto la puesta en ejecución de dichos procedimientos durante el tiempo previsto por su derecho interno.
4. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15".

La orden de conservación de datos es una medida preliminar que debe interesarse simultáneamente a la apertura del proceso penal, y a la espera de que puedan adoptarse otras medidas judiciales que permitan a la Policía acceder a los datos en cuestión. Por lo tanto, la adopción de esta medida no implica que las autoridades puedan tener acceso inmediato a cualquiera de los datos bajo custodia, sino únicamente que el poseedor de los mismos está obligado a protegerlos hasta que se produzca le medida complementaria.

El plazo máximo de custodia deberían ser suficientes para que las autoridades puedan adoptar tales medidas complementarias (el registro, el embargo o la autorización judicial de acceso a los datos como veremos más adelante)[341].

La orden de conservación de datos puede resultar esencial en las investigaciones relativas a hechos ilícitos cometidos a través de las TIC dada la vulnerabilidad de las evidencias electrónicas y la posibilidad de que sean destruidas o modificadas bien sea de forma intencional o por procesos automáticos predeterminados. Hay que tener en cuenta que las posibilidades de conservación alcanzan -con carácter cautelar y a los solos efectos anteriormente indicados- a todo tipo de tipo de datos, por cualquier tipo de delito y sea cual sea la entidad o persona física o jurídica que los tenga en su poder[342]. El requerido vendrá obligado a prestar su colaboración y a guardar secreto del desarrollo de esta diligencia, en caso contrario incurrirá en desobediencia.

Se trata de una medida importante en el marco de la cooperación internacional en la lucha contra la ciberdelincuencia, dado que la solicitud de conservación de datos puede provenir de autoridades judiciales o policiales de otros países a tenor del carácter transnacional de muchas de las actividades ilícitas que se desarrollan en el ciberespacio.

[341] Hay que puntualizar que a tenor del art. 29.7 del CSC, las solicitudes de auxilio judicial internacional relativas a una orden de conservación inmediata de datos deben ser válidas al menos durante un período de sesenta días con el fin de que la parte requirente pueda presentar una solicitud de registro, de embargo, de acceso u obtención de los datos por un medio similar, o de divulgación de los datos sometidos a conservación.

[342] TEJADA DE LA FUENTE. "La retención obligatoria de los datos de tráfico (…)". ob. cit. pág. 341. Puede dirigirse no solo a los operadores de comunicaciones sino a los proveedores de servicios de internet y, en general, a cualquier persona física y jurídica que tenga a su disposición datos de esta naturaleza.

2.5 Captación de Conversaciones Públicas.

Existen medios en internet, como los chats o foros, que permiten comunicarse a varias personas simultánea y públicamente en tiempo real. Obviamente, cuando las comunicaciones son accesibles para cualquier usuario de internet, no pueden tener la consideración de conversaciones privadas, pues es el propio usuario de la red quien se introduce en la misma y asume que muchos de los datos se convierten en públicos para todos los usuarios. Por ello, estas modalidades no pueden considerarse amparadas por el derecho fundamental al secreto de las comunicaciones, por lo que no precisan de autorización judicial para su grabación u observación, en virtud de la máxima de que "*no se precisa autorización judicial para conseguir lo que es público*" [343].

Lo mismo es predicable respecto a la intervención de comunicaciones emitidas por radiofrecuencia, que no necesita autorización judicial al quedar fuera de la reserva que establece el artículo 18.3 de la Constitución Española. Debemos llegar a esta conclusión, toda vez el texto constitucional limita su alcance a las comunicaciones secretas (esto es, reservadas), que son las únicas en las que se puede garantizar el crácter secreto que ya tienen, pero no a las comunicaciones públicas. En consecuencia, si atendemos a la naturaleza de las comunicaciones de radio que, por el medio técnico en el que se desenvuelven siempre son públicas, nunca precisarán de una autorización judicial para hacer público lo que ya lo es[344]. Tampoco en el caso de una frecuencia de radio reservada puede invocarse el secreto, exigiendo autorización judicial[345].

---

[343] SSTS 236/2008 de 9 de mayo, 292/2008 de 28 de mayo y 776/2008, de 18 de noviembre. También recoge dicho principio la STS 680/2010 de 14 de julio y la Sentencia de la Audiencia Provincial de Madrid 840/2015, de 23 de octubre (entre otras).

[344] En este sentido, señala la STS 695/2013, de 22 de julio que "*como decíamos en la STS 1397/2011 de 22 de diciembre, con citación de la STS 209/2007, de 9 de marzo, y en un supuesto muy similar al de autos, donde dicha captación tiene lugar, también en el curso de otra investigación, las captaciones de conversaciones radiotelegráficas, en frecuencia de uso público, no precisan autorización judicial, porque precisamente por ser de uso público y siendo esto conocido por los usuarios, ello implica una implícita aceptación de la posibilidad de captación".*

[345] La STS 209/2007, de 9 de marzo "la sentencia de instancia destaca que, conforme al consabido Reglamento de Radiocomunicaciones, art. S 5.2, siendo Venezuela, estado de la bandera del Buque, perteneciente a la Región 2, la frecuencia 8.760.8 es atribuida al Servicio de Navegación Aeronáutica, por lo que no podía ser utilizada por la embarcación; como tampoco la frecuencia 8.888.8 que está atribuida a los servicios de radiolocalización (de buques necesitados de socorro) de radionavegación marítima, limitada a los radares costeros. Por lo que concluye que la utilización de esas frecuencias por el buque para sus comunicaciones sería ilegal, no pudiendo invocar secreto sobre una frecuencia no hábil para ello, especialmente la atribuida a la aeronavegación".

Distinto ha de ser el tratamiento de la comunicación bidireccional cerrada entre dos usuarios, pues en estos casos, conforme a la propia naturaleza del acto comunicativo, resultan predicables las garantías del art. 18.3 CE.

2.6 Actuación en casos de urgencia.

Existen determinadas diligencias de investigación tecnológica que puede llevar a cabo la policía (por sí, u ordenadas el Ministro del Interior o el Secretario de Estado de Seguridad), sin contar *ex ante* con autorización judicial, pero cuya adopción resultará justificada cuando existan razones fundadas de urgencia. Además, las garantías procesales exigen que posteriormente dicha actuación administrativa sea convalidada mediante la necesaria autorización judicial *ex post:*

1. La interceptación de las comunicaciones telefónicas y telemáticas. En caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas y existan razones fundadas que hagan imprescindible esta medida. La diligencia podrá ordenarla el Ministro del Interior o, en su defecto, el Secretario de Estado de Seguridad.

Debe hacerse especial hincapié, por las posibles dudas de inconstitucionalidad que puede presentar el contenido del apartado 3º del artículo 588 ter d), que se habilite la posibilidad que la medida pueda acordarla el Ministro del Interior o, en su defecto, el Secretario de Estado de Seguridad y no necesariamente la autoridad judicial, ya que el artículo 18.3 CE no deja espacios intermedios a la aplicación e interpretación de dicho precepto.

No obstante, esta medida habrá de ser convalidada por el juez competente dentro del plazo máximo de 24 horas, haciendo constar las razones que justificaron su adopción, la actuación realizada, la forma en que se ha efectuado y su resultado. El juez también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de 72 horas desde que fue ordenada la medida.

2. Registro de dispositivos de almacenamiento masivo de la información[346]. En los casos de urgencia en que se aprecie un interés constitucional legítimo, la Policía Judicial podrá llevar a cabo el examen directo de los datos contenidos en el dispositivo incautado, comunicándolo inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, por escrito motivado al juez competente, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de 72 horas desde que fue ordenada la medida.

Una actuación similar se prevé respecto a los registros en la nube, ya que en caso de urgencia, la Policía Judicial podrá llevarlo a cabo, informando al juez inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, de la actuación realizada, la forma en que se ha efectuado y su resultado.

Sin embargo, no sucede lo mismo en los registros remotos pues cuando los agentes que lo llevan a cabo tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del mismo pondrán este hecho en conocimiento del juez, quien podrá autorizar una ampliación de los términos del registro[347].

Dichas actuaciones deben estar presididas por la concurrencia de los siguientes presupuestos[348]:

a) La **urgencia** en el acceso a los datos.

b) La **necesidad** de obtener la información de forma que el registro devenga estrictamente necesario para la finalidad de la investigación.

c) La **proporcionalidad** en la actuación.

[346] Artículo 588 sexies c apartados 3º y 4º.

[347] Artículo 588 septies a. apartado 3º.

[348] DELGADO MARTIN, J. "Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015". Diario La Ley, Nº 8693, Sección Doctrina, 2 de Febrero de 2016, Ed. La Ley. pág. 7

La STS 786/2015, de 4 de diciembre, se refiere a forma implícita a un supuesto de urgente intervención policial en relación con imágenes de agresiones sexuales a niñas de cinco y ocho años de edad, razonando que "*la simple posibilidad de que esas imágenes pudieran llegar a convertirse, de una u otra forma, en contenidos difundibles en la red, intensificando de forma irreparable el daño ocasionado a las dos menores, era un riesgo que había de ser ponderado en el momento del juicio de necesidad y proporcionalidad"*.

Igualmente interesante es la STS 204/2016, de 10 de marzo, respecto a un supuesto en el que la policía accedió a los teléfonos móviles de los detenidos, sin autorización judicial, extrayendo datos de la agenda que llevó a la identificación del receptor de la droga. La sentencia considera que la prueba de cargo procedente de la injerencia policial en el derecho constitucional a la intimidad sin la concurrencia de razones de urgencia y necesidad que hiciese imprescindible la intervención inmediata es nula, y sin ella la prueba de cargo concurrente para justificar la condena del recurrente es notoriamente insuficiente. En el caso concreto transcurrieron varios días desde la incautación de los teléfonos móviles hasta su manipulación y examen, considerando el TS que debería haberse puesto a disposición del Juzgado y solicitado la autorización judicial.

La doctrina del Tribunal Constitucional sostiene que la valoración de la urgencia y necesidad de la intervención policial ha de realizarse *ex ante*, y es susceptible de control judicial *ex post*, al igual que el respeto del principio de proporcionalidad. La constatación *ex post* de la falta del presupuesto habilitante o del respeto al principio de proporcionalidad implicaría la vulneración del derecho fundamental y tendría efectos procesales en cuanto a la ilicitud de la prueba en su caso obtenida, por haberlo sido con vulneración de derechos fundamentales (STC 206/2007, de 24 de septiembre y STC 70/2002, de 3 de abril).

3. TÉCNICAS DE INVESTIGACIÓN TECNOLÓGICA QUE REQUIEREN AUTORIZACIÓN JUDICIAL.

3.1 Orden en relación con la cesión de datos sobre tráfico almacenados.

3.1. A) Régimen jurídico de la cesión de datos.

En la investigación de algunos hechos delictivos puede resultar de una importancia decisiva la incorporación de los datos de tráfico o asociados. Piénsese por ejemplo, en las comunicaciones por medio de telefonía móvil o en las comunicaciones a través de internet, que generan multitud de datos referidos a los propios elementos técnicos utilizados (IP o IMEI), a la línea telefónica empleada (IMSI, número de teléfono), al propio hecho de la comunicación en sí (listados de llamadas, hora de inicio y finalización, lugar desde el que se realiza) o a las personas que intervienen en la comunicación (titular de la línea, dirección, cuenta de domiciliación de recibos).

Esta ingente cantidad de datos personales se almacenan en los archivos de los proveedores de servicios de comunicaciones electrónicas y de redes públicas de comunicaciones y se denominan "metadatos"[349].

Ya se ha dicho supra que dicha diligencia se venía practicando al amparo de lo previsto en la *Ley 25/2007, de 18 de Octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones*[350]*,* que obligó no

[349] ENCINAR DEL POZO, M Á. "La invalidez de la Directiva sobre Conservación y Cesión de los Datos relativos a las Comunicaciones ". Revista SEPIN SP/DOCT/18682, 7 de noviembre de 2014.

[350] *Vid.* Apéndice Normativo. A través de esta ley, según se destaca en su Exposición de Motivos, se llevó a efecto la transposición en nuestro ordenamiento jurídico de la *Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo sobre conservación de datos generados y tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes publicas de comunicaciones*. Directiva que fue declarada inválida el 8 abril 2014, por el Tribunal de Justicia de la Unión Europea. Se fundamenta dicha invalidez no porque no fuera posible guardar esos datos en ficheros, sino porque entiende el TJUE que conforme al contenido de la Directiva no quedaba suficientemente garantizados los derechos fundamentales de los artículos 7 (derecho a la vida privada y de las

solo a la conservación de dichos datos, sino también a su cesión a los agentes facultados (Policía Judicial, Vigilancia Aduanera y CNI) siempre que les fuesen requeridos, a través de la correspondiente autorización judicial, y con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales. Los sujetos pasivos destinatarios de esta obligación son los proveedores de servicios de internet y operadoras que prestan servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones (art. 2 de la Ley 25/2007).

De la conservación de estos datos del tráfico se excluye el contenido de la comunicación, por lo que no afecta al secreto de las comunicaciones, sino al derecho fundamental a la privacidad y a la limitación del uso de la informática, (es decir, al artículo 18, en su apartados 1 y 4 de la Constitución Española) aunque en muchas resoluciones se cite también como injerencia el artículo 18.3 de la CE. De hecho el artículo 1.3 de la Ley 25/2007 establece:

"*Se excluye del ámbito de aplicación de esta Ley el contenido de las comunicaciones electrónicas, incluida la información consultada utilizando una red de comunicaciones electrónicas*."

La Ley 25/2007 regula sólo la conservación y cesión de los datos de tráfico externos al contenido de esas comunicaciones, necesarios para rastrear e identificar el origen y destino de una comunicación de telefonía de red fija y móvil, y respecto al acceso a internet, al correo electrónico y la telefonía por internet.

Incluye dentro de su ámbito de aplicación[351] los datos necesarios para identificar el origen y destino de la comunicación, así como la identidad de los usuarios o abonados de ambos (nombre y dirección), los que permiten determinar el momento y duración, el tipo de servicio y el equipo de comunicación utilizado por los usuarios que, cuando se trate de un equipo móvil, también abarcará los datos necesarios para su

comunicaciones) y 8 (protección de los datos de carácter personal) de la Carta de los Derechos de la Unión.

[351] *Vid.* artículo 3 de la Ley 25/2007, de 18 de octubre.

localización[352]. En todo caso, la cesión de tales datos por las operadoras se subordinaba conforme al art. 1.1 de la Ley a "*la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales".*

Antes de la reforma de la LECrim de 2015, para solicitar la cesión de estos datos a los proveedores de servicios de telecomunicaciones e internet que estaban obligados a conservar, se requería autorización judicial, conforme al Acuerdo de Sala del Tribunal Supremo de 23 de Febrero de 2010:

"*Es necesaria la autorización judicial para que los operadores que prestan servicios de comunicaciones electrónicas o de redes públicas de comunicación cedan los datos generados o tratados con tal motivo. Por lo cual, el Ministerio Fiscal precisará de tal autorización para obtener de los operadores los datos conservados que se especifican en el artículo 3 de la Ley 25/2007, de 18 de octubre"*[353].

El Ministerio Fiscal precisaba también de la autorización judicial para que le fuera desvelada la identidad de la persona adjudicataria de la dirección IP con la que operan los ciudadanos en internet[354]. Debe recordarse aquí que *la Circular 1/2013 de la Fiscalía General del Estado, sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas*, declara al respecto que "*puede pues concluirse con que tras fluctuaciones jurisprudenciales se ha asentado el criterio que establece que la relación de llamadas emitidas o recibidas por un terminal telefónico es materia que afecta al derecho que garantiza el artículo 18.3 CE, siendo necesario a tales efectos, a falta de consentimiento de los sujetos comunicantes, la autorización judicial correspondiente otorgada en el curso de una investigación de carácter penal. Tal autorización será también necesaria para acceder al registro de llamadas entrantes y salientes grabadas en un teléfono móvil."*

[352] Circular 1/2013 de la Fiscalía General del Estado, sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas. De esta manera, recoge un concepto más amplio de datos, que exceden de lo que tradicionalmente se ha considerado datos externos a la comunicación amparados por el art 18.3 CE.

[353] Acuerdo plasmado posteriormente en la STS 247/2010, de 18 de marzo.

[354] STS 556/2009, de 16 de marzo.

La operadora no sólo conoce quién y desde dónde hace la llamada (SIM), sino también desde qué terminal telefónico se realizó.

Normalmente esos datos los conservará la operadora durante un año (artículo 5 Ley 25/2007), y aunque se cancelen[355], se conservarán hasta la prescripción del delito a disposición de los Tribunales.

Ni que decir tiene que si se aportara el dato conseguido sin la autorización judicial o el consentimiento investigado, la ulterior prueba sería nula por haber sido obtenida con violación del derecho a la intimidad personal del encausado.

Ahora bien, la Ley 25/2007 creó una confusión al restringir la posibilidad de cesión a *la averiguación de delitos graves*[356] del artículo 33 del Código Penal (que estaban castigados con una prisión superior a cinco años) lo que dejaba impunes múltiples ciberdelitos al impedir investigar conductas que aún utilizando tecnologías de la información y la comunicación y teniendo gran trascendencia social, no alcanzaban por la penalidad asignada la categoría de delito grave. Por ello, *la Circular 1/2013 de la Fiscalía General del Estado de 11 de enero, sobre pautas en relación con la Diligencia de intervención de las comunicaciones telefónicas,* mantuvo que una interpretación teleológica había de llevar al entendimiento de que la gravedad debía definirse en atención a las circunstancias concretas del hecho, teniendo en cuenta el bien jurídico protegido y la relevancia social de la actividad, de conformidad con la jurisprudencia

[355] Lo dispuesto anteriormente, sin perjuicio de lo previsto en el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que señala que la cancelación de los datos no supone su eliminación automática, sino su bloqueo tal y como dispone el artículo 16.3 de la Ley Orgánica 15/1999, al establecer que: "*La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión*." Es decir, la cancelación de los datos no supone su eliminación automática para los Jueces y Policía, sino sólo su bloqueo, conservándose a su disposición y por tanto, son de posible investigación criminal, para determinar y depurar las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas.

[356] La Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, *sobre conservación de datos generados y tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones* (declarada inválida el 8 abril 2014, por el Tribunal de Justicia de la Unión Europea) en su art. 1 también limitaba el acceso a los datos a la investigación de delitos graves, pero sin definir ni delimitar tal concepto, sino dejando su desarrollo al criterio de los Estados. Limitar el ámbito de la Ley a los delitos graves tal y como se definían en los arts. 13 y 33 CP supondría en realidad frustrar tanto la finalidad perseguida por la Directiva 2006/24/CE como el objetivo de la Convención sobre Ciberdelincuencia del Consejo de Europa, que es precisamente posibilitar la investigación de los delitos que se sirven de las tecnologías de la información y la comunicación.

recaída en relación con los delitos susceptibles de ser investigados mediante intervenciones telefónicas[357] .

[357] La jurisprudencia del TS había establecido que una medida de investigación judicial que afectara tan directa y gravemente a la intimidad de las personas solo podía encontrar su justificación, en el ámbito del proceso penal, cuando lo que se persiga sea un delito grave, en el bien entendido de que no sólo ha de tenerse en cuenta la gravedad de la pena, sino también su trascendencia y repercusión social (STS 740/2012, de 10 de octubre, STS 467/1998, de 3 de abril, STS 622/1998, de 11 de mayo).

La STC 104/2006, de 3 de abril, en un supuesto de investigación de hechos presuntamente constitutivos de delito contra la propiedad intelectual cometidos utilizando las tecnologías de la información consideraba admisible la diligencia de interceptación de comunicaciones, pese a que la pena establecida para este delito (art. 270 CP) era considerada en el Código penal menos grave (art. 33.2), en base a la trascendencia social y la relevancia jurídico-penal de los hechos, pues "*en el juicio de proporcionalidad de la interceptación de las comunicaciones telefónicas, además de la gravedad de la pena, del bien jurídico protegido y de la comisión del delito por organizaciones criminales, también puede ponderarse la incidencia del uso de las tecnologías de la información, pues su abuso facilita la perpetración del delito y dificulta su persecución"*.

Se había considerado que la investigación de un posible delito de robo con violencia en las personas tiene gravedad suficiente para poder acordar una intervención telefónica. La STS 1426/1998, de 23 de noviembre, declara en relación con estos delitos que "tienen una gravedad que no ha sido puesta en duda en ningún momento. Prueba de ello es que en el derecho europeo este delito aparece, por ejemplo, en la enumeración contenida en el parágrafo. 100 a 2. de la Ordenanza Procesal Alemana. Se trata, como es claro, de hechos que tienen riesgo para bienes jurídicos personales de singular importancia y que, por ello, justifican una medida como la intervención telefónica".

El delito de blanqueo de capitales también es susceptible de ser investigado a través de este medida pese a no ser delito grave. En este sentido declara la STS 960/2008, de 26 de diciembre que este delito "es en principio un delito menos grave, aunque en alguna de sus modalidades puede convertirse en grave. La lucha contra el blanqueo de capitales es hoy una de las preocupaciones preferentes de política criminal a nivel no solo europeo sino también mundial, y la dificultad de investigación por otros medios, especialmente en operaciones internacionales, con organizaciones coordinadas lo que supone altos niveles de opacidad, son criterios que deben tomarse en consideración para decidir la proporcionalidad de la medida, a lo que hay que añadir que, en este caso, dicho delito de blanqueo de capitales aparecía relacionado, en su origen, con presumibles conductas de tráfico de drogas, cuya gravedad, cuando se trata de sustancias que causan grave daño a la salud, nadie puede cuestionar. No puede hablarse, pues, de falta de proporcionalidad de la medida".

Se admite también la intervención telefónica en investigación de un delito de contrabando de tabaco (STC 14/2001, de 29 de enero; STC 202/2001, de 15 de octubre).

Del mismo modo se ha convalidado la intervención en investigación de delitos cometidos por funcionarios públicos en el ejercicio de sus cargos (STC 184/2003, de 23 de octubre) con independencia de la penalidad pues "*su relevancia estructural para el funcionamiento del Estado y la transcendencia social de los mismos al producir el socavamiento de la confianza de los ciudadanos en aquél y en sus instituciones, entre las cuales los partidos políticos son esencialmente relevantes en el marco de un sistema democrático y pluralista, avalan, sin duda, su gravedad"*. Ya el ATS de 18 de junio de 1992 consideró de suficiente gravedad los delitos cometidos por cargos públicos, por el importante deterioro social que implica esa falta a la confianza de los electores. Se ha considerado que a los efectos analizados "el delito de revelación de secretos del art. 417 CP tiene una especial gravedad, pues tiene como consecuencia la frustración de la actividad de seguridad pública del Estado" (STS 1898/2000, de 12 de diciembre).

Igualmente se ha estimado proporcional la intervención de un teléfono en el curso de una investigación que "versaba sobre la utilización de los bancos de datos personales de un organismo oficial para venderlos a terceros a cambio de un precio" (STS 1194/2004, de 7 de diciembre). También se tiene especialmente en cuenta el dato de que se investiguen organizaciones criminales (STS 960/2008, de 26 de diciembre, STS 1426/1998, de 23 de noviembre).

Actualmente, la LECrim acoge por una parte, el criterio que venía fijado en la Ley de conservación de datos, e impone la exigencia de autorización judicial para su cesión a los agentes facultados, siempre que se trate de datos vinculados a procesos de comunicación (artículo 588 ter j) y se amplía el abanico de datos, ya que no son sólo los que las operadoras tienen la obligación de conservar en cumplimiento de la Ley 25/2007, sino también a los que se conserven por propia iniciativa por motivos comerciales o de otra índole.

Además, resuelve cualquier posible controversia respecto a la penalidad del delito, pues desaparece la exigencia de que sea un delito "grave" para la adopción de la medida. Esto es, podrá ser autorizada cuando el conocimiento de esos datos resulte indispensable para la investigación, que tenga ésta además por objeto alguno de los delitos a que se refiere el artículo 579.1 LECrim (*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)* o delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o servicio de comunicación.

Ahora bien, hay que hacer referencia a la cuestión prejudicial planteada por la Sección Cuarta de la Audiencia Provincial de Tarragona mediante Auto de 6 de abril de 2016[358] para que el Tribunal de Justicia de la Unión Europea se pronuncie expresamente

---

Incluso se ha convalidado una intervención ante un delito de hurto, atendiendo a las circunstancias concurrentes. La STS 126/2000, de 16 mayo declara al respecto que "*la comprobación de la proporcionalidad de la medida ha de construirse….analizando las circunstancias concurrentes en el momento de su adopción. Desde ese punto de vista no se aprecia que la medida acordada por el Juez fuera desproporcionada. En primer lugar, porque… se trató de una investigación de un delito de hurto, en cantidad de especial y cualificada gravedad…y continuado…Se aprecia por tanto que, en el momento en que los órganos judiciales adoptaron la medida, la infracción podía no ser calificada como leve. A esta misma conclusión se llega si se tienen en cuenta las especiales circunstancias concurrentes en el caso (posible infidelidad de una parte de los empleados del almacén de la empresa denunciante, y gran dimensión de la empresa) y muy especialmente la no despreciable posibilidad de continuación del hecho delictivo en curso".*

En los supuestos examinados que se trataba además de validar la intervención de las comunicaciones, esto es, una injerencia en el contenido de lo comunicado, de mayor entidad que la averiguación de meros datos externos. Una interpretación sistemática conduce a la misma conclusión: ningún sentido tendría imponer mayores restricciones a la cesión de datos externos que al acceso al contenido de lo comunicado. Por ello, al margen de que los Sres. Fiscales defiendan *de lege data* la interpretación superadora de la literalidad del precepto, es a todas luces aconsejable *de lege ferenda* la modificación de la Ley 25/2007 para sustituir la expresión "delito grave" por otra que delimite el perímetro de aplicación de la Ley en términos más amplios y razonables.

[358]Rollo de apelación penal 628/2015, Sección 4ª de la Audiencia Provincial de Tarragona, dimanante del procedimiento abreviado 689/2015 del Juzgado de Instrucción número 3 de Tarragona.

sobre si la reforma de la LECrim en cuanto a la cesión de datos es compatible con las exigencias contenidas en la STJUE de 8 de abril de 2014 que anuló la Directiva 2006/24/CE, en lo relativo a la gravedad del delito y al umbral mínimo de la pena a imponer y si éste es compatible con tres años de prisión.

Mi criterio al respecto es que en la investigación del ciberdelito resulta indispensable contar con la colaboración de los ISP para la cesión de los datos almacenados pues es el primer paso en la investigación y, en la mayor parte de los casos, es esencial para averiguar la autoría. Estos datos han de ser cedidos con independencia de la penalidad señalada al ciberdelito ya que entenderlo de otra manera sería dejar en la impunidad a un gran número de delitos. Todo ello, sin olvidar que la resolución judicial necesaria para autorizar la cesión de los datos ha de realizar un juicio de ponderación entre el derecho fundamental afectado y la finalidad perseguida. La autorización y control individualizado por parte de la autoridad competente de todos aquellos supuestos en los que se quiere hacer uso de esa información es el mejor y más seguro filtro para analizar la entidad de la conducta investigada, su gravedad, su trascendencia, la necesidad de dicha información a efectos de investigación criminal y en definitiva, la proporcionalidad del acceso solicitado[359].

El hecho investigado es el robo con violencia de un teléfono móvil. Para investigar la autoría la policía solicitó al Juez Instructor que se librase mandamiento a las operadoras para que informasen y en su caso remitiesen los datos de la persona que tras el robo activó una tarjeta SIM con el IMEI del terminal sustraído. El Juez de Instrucción denegó la medida al entender que el delito investigado no tenía prevista una pena de prisión superior a 5 años (no se investigaba un delito grave). Tal decisión fue recurrida por la Fiscalía alegando la doctrina jurisprudencial que estimaba que para calibrar la gravedad no hay que estar únicamente a la gravedad de la pena prevista, sino a otros indicadores como la importancia del bien jurídico afectado o la trascendencia social del delito que se investiga. La Audiencia, antes de decidir sobre el particular, y valorando que ya había entrado en vigor la Ley Orgánica 13/2015 (en concreto, tal reforma había dejado en papel mojado la limitación de la Ley 25/2007 que pivotaba sobre la gravedad de la pena, e introducido otros criterios en el artículo 588 ter a en relación con el artículo 579.1 de la LECrim que en la práctica pueden llevar a la autorización de la cesión de datos en la investigación de cualquier delito independientemente de la gravedad de la pena que tenga prevista), decidió que debía plantear una cuestión prejudicial ante el Tribunal de Justicia de la Unión Europea, sobre estos extremos: *¿La suficiente gravedad de los delitos como criterio que justifica la injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta, puede identificarse únicamente en atención a la pena que pueda imponerse al delito que se investiga o es necesario, además, identificar en la conducta delictiva de particulares niveles de lesividad para bienes jurídicos individuales y/o colectivos?*
o En su caso, si se ajustara a los principios constitucionales de la Unión, utilizados por el TJUE en su sentencia de 8 de abril de 2014 como estándares de control estricto de la Directiva, la determinación de la gravedad del delito, atendiendo solo a la pena imponible, cuál debería ser ese umbral mínimo? ¿Sería compatible con una previsión general de límite en tres años de prisión?

[359] TEJADA DE LA FUENTE, E. "La retención obligatoria de los datos de tráfico (…)". ob. cit. pág. 333.

3.1.B) Procedimiento de cesión de datos conservados.

La LECrim y los artículos 6 y 7 de la Ley de Conservación de Datos regulan el procedimiento de cesión de los datos conservados obligando a ello a los operadores siempre que exista resolución judicial. El procedimiento de cesión de datos, desde la solicitud y las actuaciones posteriores relativas a la medida solicitada, se sustanciarán en una pieza separada y secreta, sin necesidad de que se acuerde expresamente el secreto de la causa, de conformidad con el artículo 588 bis d de la LECrim.

3.1.B. 1) Solicitud de cesión de datos.

La LECrim considera adecuado no abandonar los aspectos formales de la solicitud y del contenido de la resolución judicial habilitante. La práctica forense no es ajena a casos de solicitudes policiales y de ulteriores resoluciones judiciales que adolecen de un laconismo argumental susceptible de vulnerar el deber constitucional de motivación. A fin de evitar ese efecto se orienta la minuciosa regulación del contenido de esa solicitud, así como de la resolución judicial que, en su caso, habilite la medida de injerencia.

La solicitud podrá acordarse de oficio o a instancia del Ministerio Fiscal o de la Policía Judicial. En este último caso la solicitud deberá contener[360]:

1º. La descripción del hecho objeto de investigación y la identidad del investigado o de cualquier otro afectado por la medida, siempre que tales datos resulten conocidos.

2º. La exposición detallada de las razones que justifiquen la necesidad de la medida de acuerdo a los principios rectores establecidos en el artículo 588 bis a, así

[360] Artículo 588 bis b. 2. Solicitud de autorización judicial. (común a todas las técnicas de investigación previstas en este epígrafe).

como los indicios de criminalidad que se hayan puesto de manifiesto durante la investigación previa a la solicitud de autorización del acto de injerencia.

3º. Los datos de identificación del investigado o encausado y, en su caso, de los medios de comunicación empleados que permitan la ejecución de la medida.

4º. La extensión de la medida con especificación de su contenido.

5º. La unidad investigadora de la Policía Judicial que se hará cargo de la intervención.

6º. La forma de ejecución de la medida.

7º. La duración de la medida que se solicita.

8º. El sujeto obligado que llevará a cabo la medida, en caso de conocerse.

3.1.B. 2)Resolución judicial.

La resolución judicial que autoriza o deniega la solicitud adoptará la forma de auto motivado y deberá dictarse en el plazo de 24 horas desde que se presentó la solicitud, aunque el Juez podrá requerir con interrupción del plazo legal la ampliación o aclaración de sus términos (artículo 588 bis c).

El auto deberá contener, el hecho punible objeto de investigación y su calificación jurídica, con expresión de los indicios racionales en los que funde la medida, además de exteriorizar los datos o hechos objetivos que pueden considerarse indicios de la existencia del delito y de la conexión de la persona o personas investigadas con el mismo[361]. Pero no se puede confundir que se requieran datos para ordenar la injerencia, a que desde el primer momento queden ya acreditados los hechos

[361] (SSTC 25/2011, de 14 de marzo; 70/2010, de 18 de octubre; 197/2009, de 28 de septiembre; 184/2003, de 23 de octubre y 167/2002, de 18 de septiembre).

que precisamente se van a comenzar a investigar[362]. Se trata de una medida adoptada, precisamente, para profundizar en una investigación no acabada por lo que únicamente pueden conocerse unos iniciales elementos indiciarios (STS 740/2012, de 10 de octubre). Se exige que concurran indicios de criminalidad sobre la persona a la que va a afectar la medida limitadora del derecho fundamental, partiendo lógicamente de que se trata de hacer acopio de elementos incriminadores de los que hasta ese momento se carece[363].

Deben concurrir datos o hechos objetivos que puedan considerarse indicios de la existencia del delito y la conexión de la persona o personas investigadas con el mismo[364]. Los indicios que se exigen son algo más que simples sospechas, pero también algo menos que los indicios racionales que se exigen para el procesamiento[365].

---

[362] La STS 203/2015, de 10 de marzo, precisa que "*naturalmente, no pueden utilizarse datos que no consten en tales oficios, pero tampoco puede exigirse verificaciones añadidas a lo expuesto en el oficio policial; podrán solicitarse nuevos datos, dictando una resolución judicial para que se amplíen los elementos indiciarios expuestos, pero no puede exigirse prueba de los que allí figuran, puesto que de las afirmaciones que consten en el informe policial ha de partir el juez para verificar el juicio de proporcionalidad, idoneidad y necesidad*" (en el mismo sentido, STS 246/2014, de 2 de abril)

[363] Como atinadamente expresa la STS 926/2007, de 13 de noviembre, lo exigible en esta fase no es, desde luego, la aportación de un acabado cuadro probatorio. Pero sí que se pongan a disposición del juez aquellos elementos de juicio en virtud de los cuales la policía ha podido llegar, de forma no arbitraria, a la conclusión de la necesidad de implantar una medida tan grave (referida a la intervención de comunicaciones).

[364]El Instructor ha de sopesar el grado de probabilidad que se deriva de los indicios. Sólo cuando éste adquiera ciertas cotas que sobrepasen la mera posibilidad, estará justificada la injerencia. No basta una intuición policial; ni una sospecha más o menos vaga; ni deducciones basadas en confidencias. (STS 658/2012, de 13 de julio).

[365] STC 26/2010, de 27 de abril *"(...)Esto es, sospechas fundadas en alguna clase de datos objetivos, que han de serlo en un doble sentido: en el de ser accesibles a terceros, sin lo que no serían susceptibles de control; y en el de que han de proporcionar una base real de la que pueda inferirse que se ha cometido o que se va a cometer el delito, sin que puedan consistir en valoraciones acerca de la persona. Han de excluirse las investigaciones meramente prospectivas, pues el secreto de las comunicaciones no puede ser desvelado para satisfacer la necesidad genérica de prevenir o descubrir delitos o para despejar las sospechas sin base objetiva que surjan de los encargados de la investigación, ya que de otro modo se desvanecería la garantía constitucional; exclusión que se extiende igualmente a las hipótesis subjetivas y a las meras suposiciones y conjeturas, pues si el secreto pudiera alzarse sobre la base de esas hipótesis, quedaría materialmente vacío de contenido"* (en el mismo sentido las SSTC 5/2010, de 7 de abril, 197/2009, de 28 de septiembre y 253/2006, de 11 de septiembre).
En relación a los indicios en relación a la intervención de comunicaciones, señala la STS 153/2015, de 18 de marzo que "*los indicios se piden para justificar el sacrificio del derecho fundamental a la privacidad de las conversaciones pero no constituyen ni se equiparan al concepto de indicios que se utiliza en el art. 384 LECrim El "indicio racional de criminalidad" al que se refiere el art. 384 de la LECrim para el procesamiento que constituye un "juicio de probabilidad" sobre el delito ya investigado, y sobre la implicación de la persona procesada en él. Es en definitiva un juicio provisional de inculpación que descansa sobre la totalidad de la encuesta judicial ya efectuada. En el caso de la petición de intervención telefónica se está en una fase muy anterior, pues la investigación judicial prácticamente no ha empezado,*

Estos indicios han de contar con cierto fundamento de investigación identificable y susceptible de ulterior contrastación, que es lo que los distingue de las "meras hipótesis subjetivas"[366]. Son válidas las máximas de experiencia como indicios[367] y las informaciones confidenciales[368] y los indicios proporcionados por policías extranjeras[369].

---

por tanto los "indicios" justificadores de la petición de intención, se sitúan, como con reiteración ha dicho tanto esta Sala como el Tribunal Constitucional en una zona intermedia "....son algo más que simples sospechas, pero también algo menos que los indicios racionales que se exigen para el procesamiento....".

[366] En la terminología del TEDH, se deben facilitar por la autoridad policial las "buenas razones" o " fuertes presunciones " a que dicho Tribunal se refiere en los casos Lüdi c. Suiza 15 de junio de 1992 , o Klass c. Alemania de 6 de septiembre de 1978.

[367] Establece la STS 153/2015, de 18 de marzo que "*recordemos que las máximas de experiencia también llamadas en el derecho anglosajón estándares de actuación son juicios hipotéticos de contenido general independientes del caso concreto a decidir en el proceso, y que han sido adquiridos mediante la verificación de su reiteración en el tiempo aunque son autónomos de los casos singulares de cuya observación se infieren. Vienen a ser un juicio lógico obtenido del examen de casos semejantes, y que tienen el valor de juicios, reglas o normas de comportamiento que tienen un valor complementario pudiendo ser utilizadas por el Juez. Obviamente no son verdades urbi et orbe aplicables al caso concreto, pero sí tienen el valor de ser un criterio de interpretación que con carácter auxiliar pueden ayudar al Juez en la toma de su decisión teniendo el valor de corroborar la decisión adoptada por el Juez en el caso concreto -entre otras, SSTS 343/2014, así como las anteriores 190/2013 ó 220/2013 -. El propio ordenamiento jurídico les da reconocimiento como se puede verificar en el art. 384 de la LEC cuando se nos dice que el Tribunal valoró los dictámenes periciales según las reglas de la sana crítica."*

[368] Señala la STS 704/2016, de 14 de septiembre establece que "*Las noticias o informaciones confidenciales aunque se consideran fidedignas no pueden ser fundamento, por sí solas, de una medida cautelar o investigadora que implique el sacrificio de derechos fundamentales. Pero pueden utilizarse como indicio justificativo de las escuchas si aparecen corroboradas por una investigación en la que se acopien otros significativos indicios"*.
Esas informaciones confidenciales pueden sumarse al resto de indicios recabados durante esa investigación que confirmen su fiabilidad. Algunas conductas externas pueden obedecer a mil razones diferentes la mayoría de las cuales no guardan la más mínima relación con una actividad delictiva. Su valoración será ambivalente. Pero cuando confluyen varias y adquieren plena coherencia y explicación si se ponen en relación con las informaciones confidenciales que la policía relata haber recibido, éste no es un dato neutro: es un indicio más que adquiere mayor valor por esos puntos de confirmación.

[369] Cuando los datos objetivos valorables como indicios son proporcionados a las Fuerzas y Cuerpos de Seguridad españoles por cuerpos policiales extranjeros, no es preciso acreditar la fuente de conocimiento de la policía extranjera, bastando con una mínima comprobación de tales datos por la unidad policial española. En este sentido, señala la STS 251/2014, de 13 de abril que "*cuando estas fuentes de conocimiento externo de la solicitud de nuestros servicios policiales proceden, como en este caso, de investigaciones legalmente practicadas por servicios policiales extranjeros, afirma la STS 635/2012 de 17 de julio, que cita "se debe consignar en la solicitud, además de las investigaciones internas de corroboración que se hayan podido practicar, la totalidad de los datos que los servicios policiales del país de procedencia de la droga hayan proporcionado, cuya fiabilidad debe ser valorada por el propio Juez Instructor en función de: 1º) Los datos objetivos existentes y su concreción, 2º) Los cauces oficiales de recepción y verificación de la información, 3º) Las posibilidades de confirmación interna de los aspectos periféricos de la investigación, 4º) La verosimilitud de la información y 5º) Sus propias normas de experiencia"*. Como dijo la STS 884/2012, de 12 de noviembre, "cuando servicios de información extranjeros proporcionan datos a las fuerzas y cuerpos de seguridad españoles, la exigencia de que la fuente de conocimiento precise también sus propias fuentes de conocimiento, no se integra en el

Por último, el éxito posterior de la investigación no convalida la falta inicial de indicios[370], ni la nulidad de la medida de investigación tecnológica por no existir suficientes indicios, ha de extenderse siempre a la prueba refleja[371].

Siguiendo con el contenido del auto autorizante de esta medida, deberá expresar:

a) La identidad de los investigados y de cualquier otro afectado por la medida, de ser conocido.
b) La extensión de la medida de injerencia, especificando su alcance así como la motivación relativa al cumplimiento de los principios rectores establecidos en el artículo 588 bis a. Es decir, con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida.
c) La unidad investigadora de Policía Judicial que se hará cargo de la intervención.
d) La duración de la medida.
e) La forma y la periodicidad con la que el solicitante informará al juez sobre los resultados de la medida.
f) La finalidad perseguida con la medida.
g) El sujeto obligado que llevará a cabo la medida, en caso de conocerse, con expresa mención del deber de colaboración y de guardar secreto, cuando proceda, bajo apercibimiento de incurrir en un delito de desobediencia.

---

contenido del derecho a un proceso con todas las garantías. Lo decisivo, además de la constancia oficial, no necesariamente documentada, de que esa comunicación se produjo, es que el intercambio de datos sirva para lo que puede servir, esto es, para desencadenar una investigación llamada a proporcionar a los Tribunales españoles los medios de prueba precisos para el enjuiciamiento de los hecho" (en el mismo sentido, STS 795/2014, de 20 de noviembre).

[370] La STS 203/2015, de 10 de marzo precisa que "*el éxito posterior de la investigación, tampoco puede convalidar lo que en sus raíces nacía podrido: se trata de un juicio ex ante* (STC 165/2005, de 20 de junio o STC 259/2005, de 24).

[371] Señala la STS 811/2012, de 30 de octubre que "*aunque la necesidad de tutela del derecho fundamental al secreto de las comunicaciones telefónicas es especialmente intensa, de lo expuesto en la STC 81/98 se desprende que cuando no nos encontremos ante una injerencia llevada a cabo sin intervención judicial, ni ante una intervención acordada por resolución absolutamente inmotivada, sino ante una resolución judicial en que la expresión de sus fundamentos justificativos haya sido declarada insuficiente, la necesidad de tutela inherente al derecho al secreto de las comunicaciones puede quedar satisfecha sin que resulte necesario extender dicha prohibición a las pruebas derivadas".*

h) Y el plazo de ejecución de la orden de cesión, que será fijado atendiendo a la urgencia de la cesión y a los efectos de la investigación de que se trate, así como a la naturaleza y complejidad técnica de la operación. Y en el caso de que no se establezca plazo, la cesión deberá efectuarse dentro de los 7 días naturales contados a partir de las 8.00 horas del día natural siguiente a aquél en que el sujeto reciba la orden.

La cesión de los datos se efectuará mediante formato electrónico únicamente a los agentes facultados, y deberá limitarse a la información que resulte imprescindible para la averiguación del delito.

3.2 La interceptación de las comunicaciones telemáticas como vía de investigación criminal de los ilícitos que se cometen a través de la red.

3.2.A) Marco Jurídico.

Una de las diligencias de investigación más invasivas en el ámbito de los derechos fundamentales y más compleja en su adopción, ejecución y aportación al acto del juicio oral es la de intervención de las comunicaciones telemáticas[372], pues supone la interceptación y recopilación instantáneas de datos tráfico y de contenido.

Hasta la reforma de la LECrim de octubre de 2015, la normativa que se aplicaba era el artículo 579 de la LECrim sobre detención, interceptación y observación de comunicaciones, completada con la doctrina consolidada del Tribunal Supremo y del

[372] Circular 1/2013 sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas. Ya la Fiscalía General del Estado dedicó a la materia su Circular 1/1999, de 29 de diciembre, *sobre la intervención de las comunicaciones telefónicas en el seno de los procesos penales.* El tiempo transcurrido y la evolución jurisprudencial en una materia extraordinariamente movediza y que se proyecta sobre una realidad profundamente afectada por los avances técnicos hacen necesario un nuevo pronunciamiento. En la presente Circular se incorporan las pautas exegéticas que se consideran suficientemente consolidadas en la doctrina del TC y en la jurisprudencia del TS, dejando para futuros instrumentos aspectos sobre los que aún se carece de criterios firmes y claramente asentados.

Tribunal Constitucional sobre esta materia[373]. Con esta base el TC (*vid*. STC 184/2003, de 23 octubre) echó en falta la regulación del plazo máximo de duración de las intervenciones, la delimitación de la naturaleza y gravedad de los hechos en virtud de cuya investigación podían acordarse, el control del resultado de las intervenciones telefónicas y de los soportes en los que conste dicho resultado; es decir, las condiciones de grabación, y custodia, utilización y borrado de las grabaciones, y las condiciones de incorporación a los atestados y al proceso de las conversaciones intervenidas.

Para que la intervención telefónica fuera una simple "afectación" y no "vulneración" de un derecho fundamental era preciso el escrupuloso respeto de las garantías, de modo que toda intervención era tratada como excepcional, y rodeada de límites y requisitos.

Los requisitos básicos que conforme a la jurisprudencia del TS han de concurrir para la legitimidad y validez de las intervenciones telefónicas, son los siguientes[374]:

1º) La exclusividad jurisdiccional, en el sentido de que únicamente por la autoridad judicial se pueden establecer restricciones y derogaciones al derecho al secreto de las comunicaciones telefónicas.

2º) La finalidad exclusivamente probatoria de las interceptaciones para establecer la existencia de delito y el descubrimiento de las personas responsables del mismo.

3º) La excepcionalidad de la medida, que sólo habrá de adoptarse cuando no exista otro medio de investigación del delito, que sea de menor incidencia y causación de daños sobre los derechos y libertades fundamentales del individuo que los que inciden sobre la intimidad personal y el secreto de las comunicaciones.

---

[373] Así, puede afirmarse que las exigencias establecidas en nuestro ordenamiento para las intervenciones telefónicas son de las más estrictas que existen en el ámbito del derecho comparado, en primer lugar porque en muchos ordenamientos de nuestro entorno no se exige autorización judicial, siendo suficiente la intervención de una autoridad gubernativa, y en segundo lugar porque en aquellos en que se exige la autorización judicial, generalmente ordenamientos de corte anglosajón, no se imponen al Juez las exigencias de motivación establecidas por nuestra jurisprudencia (STS 635/2012, 17 de julio).

[374] ATS de 8 de junio de 1992, STS 25 de junio de 1993 (rec. 2907/1991), SSTS 1038/1994 de 20 de mayo, 1579/1994 de 12 de septiembre, 914/1996, 20 diciembre, 988/2003 de 4 de julio y 530/2004 de 29 de abril, 960/2008, de 26 de diciembre, entre otras muchas.

4º) La proporcionalidad de la medida, que implica que sólo habrá de adoptarse en el caso de delitos graves.

5º) La limitación temporal de la utilización de la medida.

6º) La especialidad del hecho delictivo que se investigue, pues no cabe decretar una intervención telefónica para tratar de descubrir de manera general e indiscriminada actos delictivos.

7º) La existencia previa de indicios de la comisión de delito y no meras sospechas o conjeturas.

8º) La existencia previa de un procedimiento de investigación penal, aunque cabe que la intervención de las telecomunicaciones sea la que ponga en marcha el procedimiento, en los casos de hallazgo casual.

9º) La motivación suficiente de la resolución judicial acordando la intervención telefónica.

10º) La exigencia de control judicial en la ordenación, desarrollo y cese de la medida de intervención.

La exigencia del cumplimiento de estos requisitos ineludibles para que las intervenciones sean legítimas deriva, no solamente del carácter de derecho fundamental del secreto de las comunicaciones, sino además, de una singularidad que concurre respecto de otras diligencias de investigación intrusivas en los derechos fundamentales; a saber, que se lleva a cabo manteniendo al titular de ese derecho en la total ignorancia respecto a la injerencia en su derecho constitucional.

El CSC preveía la obtención e interceptación de datos de tráfico (art. 20) y de datos de contenido (art. 21)[375] en tiempo real, asociados a específicas comunicaciones en el territorio nacional transmitidas por medio de un sistema informático, tanto

[375] La distinción entre telecomunicaciones y comunicaciones informáticas y las diferencias entre sus infraestructuras está desdibujado con la convergencia de la telecomunicación y las tecnologías de la información. Es por ello, que los artículos 20 y 21 se aplican a comunicaciones específicas transmitidas por medio de un sistema informático, el cual incluye la transmisión de la comunicación a través de la red de telecomunicación antes de que sea recibido por otro sistema informático.

directamente por las autoridades competentes a través de una aplicación de medios técnicos, como obligando a un proveedor de servicios, dentro de su capacidad técnica, a obtenerlos y grabarlos o a cooperar y asistir a las autoridades competentes en la obtención y grabación.

La jurisprudencia había avalado la intervención de las comunicaciones telemáticas[376]poniendo de manifiesto la orfandad legislativa en diversas ocasiones[377].

La LECrim se refiere también específicamente a esta materia conteniendo una regulación detallada de la interceptación de comunicaciones telefónicas y telemáticas acorde a las exigencia del Tribunal Constitucional ("*Interceptación de las comunicaciones telefónicas y telemáticas"* arts. 588 ter, letras a) a i) LECrim).

3.2.B) Ambito de aplicación de la interceptación de las comunicaciones.

La autorización para la interceptación de las comunicaciones telefónicas y telemáticas solo podrá ser concedida cuando la investigación tenga por objeto alguno de los delitos a los que se refiere el artículo 579.1 LECrim (*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)* a los que se suman los cometidos por medio de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación.

[376] La STS 877/2014, de 22 de diciembre, tras valorar que "el Juez de Instrucción dictó auto autorizando la intervención de la comunicaciones telemáticas que se pudieran producir a través de la línea ADSL asociada al número de teléfono fijo citado, incluyendo los datos asociados a la comunicación, es decir, las comunicaciones de voz y el envío y recepción de correos electrónicos. La interceptación afecta, por tanto, a cualquier comunicación que tenga como origen o destino el terminal específico que se determine en el auto de intervención concluye que cumple suficientemente con las exigencias de motivación".

[377] STS 850/2014, de 26 de noviembre, "La intervención de las comunicaciones telemáticas carece de regulación legal expresa en nuestro ordenamiento procesal penal, (...) que es preciso subsanar con la máxima urgencia, dada la relevancia de los derechos fundamentales e intereses generales en conflicto. La doctrina jurisprudencial ha realizado un considerable esfuerzo para subsanar este déficit, que afecta a la calidad democrática de nuestro sistema de investigación penal, por la vía de la asimilación de las comunicaciones telemáticas al régimen de las intervenciones telefónicas, lo que implica, con carácter general, la exigencia de autorización judicial sujeta a los principios de especialidad, excepcionalidad, idoneidad necesidad y proporcionalidad de la medida"

La reforma de la LEcrim de 2015 confiere sustantividad propia a otras formas de comunicación telemática que habían carecido de tratamiento normativo en la ley procesal. Las dificultades asociadas a ese vacío legal se habían visto multiplicadas en la práctica por una interpretación jurisprudencial llamada a reglar la obligación de las operadoras de conservar los datos generados por las comunicaciones electrónicas, que habían degradado los muy extendidos instrumentos de comunicación telemática (por ejemplo, los mensajes de SMS o el correo electrónico) a la condición de aspectos accesorios, de obligado sacrificio siempre que se adopte una decisión jurisdiccional de intervención telefónica.

Frente a esta concepción, la LECrim autoriza hoy la intervención y registro de las comunicaciones de cualquier clase que se realicen a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual. Pero somete la interceptación de todas ellas a los principios generales que el texto proclama. Se pretende que sea el propio juez, ponderando la gravedad del hecho que está siendo objeto de investigación el que determine el alcance de la injerencia del Estado en las comunicaciones particulares.

La resolución habilitante deberá precisar el ámbito objetivo y subjetivo de la medida. Es decir, tendrá que motivar, a la luz de aquellos principios, si el sacrificio de las comunicaciones telefónicas no es suficiente y si la investigación exige, además, la interceptación de los SMS, MMS o cualquier otra forma de comunicación telemática de carácter bidireccional[378].

El artículo 588 ter b es el dedicado ámbito de aplicación y trasciende al del teléfono móvil, pues, alude expresamente a *"terminales o medios de comunicación telemática"*, por lo que también podrán intervenirse dispositivos como tabletas, relojes inteligentes, etc, y medios de comunicación como correos electrónicos o servicios de mensajería instantánea (*sms, mms, whatsapp, line*,...)[379]. Por tanto, mediante autorización judicial se podrá acceder tanto al propio contenido de las comunicaciones como a los datos de tráfico generados en dicha comunicación.

[378] Apartado IV del Preámbulo de la *Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.*

[379] GIMENO BEVIÁ, J. "Análisis crítico de la reforma de la LECrim 2015". Revista Aranzadi de Derecho y Proceso Penal nº 40, 2015 (Octubre-Diciembre)Legislación, pág. 9.

1) Medios de Comunicación objeto de Intervención:

Podrán intervenirse los medios de comunicación habitual u ocasionalmente utilizados por el investigado en los que participe como emisor o receptor. E igualmente podrán intervenirse los terminales o medios de comunicación de la víctima cuando sea previsible un grave riesgo para su vida o integridad.

Entre los medios de comunicación que puede ser objeto de intervención, cabe distinguir:

a) Correo Electrónico.

El correo electrónico es un medio de comunicación usual hoy día, y los concretos mensajes a través del mismo son genuinos actos de comunicación. Cuando un mensaje se envía es transmitido por el proveedor de servicios del remitente al proveedor de servicios del destinatario, quien una vez recibido lo almacena en su buzón hasta su apertura. El destinatario tiene acceso al mensaje y determina cuánto tiempo permanecerá en el buzón. Los mensajes del buzón están por consiguiente bajo el control tanto del destinatario como del proveedor y generalmente las autoridades encargadas de aplicar la ley podrían tener acceso ejerciendo medidas coercitivas contra cualquiera de ellos. Normalmente preferirán ejercerlas contra el proveedor de servicios de internet, dado que de ese modo no alertarían al destinatario sobre la existencia de la investigación.

Desde un punto de vista técnico cabe diferenciar dos partes en un correo electrónico: el cuerpo y las cabeceras. El cuerpo está formado por el contenido del mensaje en sí (incluyendo posibles adjuntos, previamente tratados por el programa de correo para poderse transmitir), y por tanto depende por completo de lo que el usuario haya decidido incluir en dicho mensaje. Mientras que las cabeceras contienen

información tanto facilitada de una u otra forma por el usuario (asunto, destinatario, emisor...) como añadida por el servidor o servidores por los que pasa el mensaje hasta llegar a su destino[380].

Por lo que respecta a la naturaleza jurídica del correo electrónico, puede decirse que antes de la reforma de la LECrim, existía una *communis opinio* en orden a considerar al *e-mail* como un medio asimilable al teléfono, a efectos de aplicarle idénticas garantías procesales penales[381]. A estos efectos, se señalaba que el e-mail era más "electrónico" que "correo". La tesis de la asimilación al teléfono se reforzaba si se reparaba en el soporte o vía por la que discurren los contenidos: la propia línea telefónica. La otra alternativa era aplicarle a toda la mensajería (correo electrónico, instantánea, sms etc..) el régimen jurídico de la intervención de la correspondencia postal, pero esta tesis era difícilmente asumible pues se hacía necesario citar al interesado para acceder a su contenido, lo que obviamente conducía al truncamiento de la diligencias.

Finalmente, la equiparación del correo electrónico al teléfono ha sido la tesis adoptada en la LECrim, pues en el capítulo relativo a la apertura de la correspondencia, el artículo 579 deja fuera al correo electrónico y se ocupa solamente de regular la correspondencia escrita o telegráfica; en concreto, dispone el precepto que el juez podrá acordar la detención de la correspondencia privada, postal y telegráfica, incluidos faxes, burofaxes y giros, que el investigado remita o reciba, así como su apertura o examen, si hubiera indicios de obtener por estos medios el descubrimiento o la comprobación del algún hecho o circunstancia relevante para la causa. Como se aprecia, no aparece el correo electrónico en esa enumeración, sino que se ha optado por incluirlo en el

[380] Estas cabeceras son importantes para determinar los datos de tráfico y algunos aspectos relevantes en relación con la investigación de la autoría de los correos electrónicos; en especial para conocer el origen, el destino y el camino que un mensaje ha seguido entre emisor y receptor, ya que cada vez que el mensaje pasa por un servidor de correo éste añade un campo de datos a las cabeceras, con etiqueta Received, especificándose el nombre del servidor, su dirección IP, el servidor de correo utilizado, y la fecha y la hora en que se emitió y se recibió el mensaje.
Estudiando detenidamente las cabeceras de un mensaje de correo electrónico se puede determinar por qué servidores de correo ha transitado dicho mensaje. Además en los servidores por donde ha transitado, es posible determinar los clientes que se han descargado el mensaje o que lo han reenviado, se puede determinar si un correo proveniente de un cierto dominio de internet se ha procesado efectivamente en servidores relacionados con dicho dominio o por el contrario viene de sistemas que a priori no son propios del mismo, lo que indicaría que el mensaje puede haber sido falseado.

[381] Circular 1/2013 de la Fiscalía General del Estado, sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas.

Capitulo V del Titulo VIII donde se regula la intervención telefónica y telemática conjuntamente otorgándole las mismas garantías procesales. A estos efectos debe aplicarse el mismo régimen a las diversas modalidades de mensajería instantánea (*instant messaging*) cuyo uso generalizado ha colocado a este medio en pieza esencial en las comunicaciones interpersonales (*ej: whatsapp* o *messenger*).

El acceso a un correo electrónico que aún no ha sido leído por su receptor, con independencia del momento concreto del proceso de comunicación en que se encuentre (ya esté escrito y almacenado en el ordenador personal, o en el terminal telefónico pendiente de ser enviado a su destinatario final, o enviado y recibido pero aún no leído), supone sin duda una injerencia en el secreto de las comunicaciones. La precitada circular 1/2013 de la Fiscalía General del Estado, sostiene que "*Debe considerarse la necesaria autorización judicial para acceder a cualquier mensaje enviado por correo electrónico, ya se trate de correo electrónico enviado y recibido pero no leído, correo en fase de trasferencia o correo ya enviado, recibido y leído y que se encuentra almacenado".*

La intervención del correo electrónico exige que la resolución judicial especifique las concretas cuentas de correo afectadas, no siendo una buena práctica la de reseñar la línea telefónica habitualmente utilizada por el sujeto pasivo de la medida, ya que el mismo puede acceder a su cuenta o cuentas de correo electrónico a través de otras líneas[382].

El principal problema radica en que gran cantidad de ISP tienen su sede en el extranjero, principalmente en EEUU, y sobre todo en que los datos que poseen se encuentran ubicados en servidores informáticos fuera del territorio español, para cuya

[382] En lo que se refiere al método -procedimiento- o los pasos a dar para la ejecución de la injerencia del correo electrónico, indicar que técnicamente la intervención se realiza configurando el servidor a través de su administrador (ISP) para reenviar el correo electrónico, monitorizando o duplicándolo sin interrumpirlo, a otra cuenta de correo electrónico autorizada en la que lo conoce el agente investigador facultado por el mandamiento Judicial. Para simplificar el análisis de la información interceptada y a la vez realizar intromisiones menos indiscriminadas que garanticen el derecho al secreto de terceros, a veces se acompaña la interceptación del uso de filtros que seleccionan los correos electrónicos, bien por su contenido, bien por su origen o destino.

consecución es prácticamente obligado solicitarlos mediante la oportuna comisión rogatoria internacional, lo que generalmente ralentiza, si no inutiliza, la investigación[383].

La mayor parte de las cuentas de correo electrónico usadas para delinquir son las gratuitas que proporcionan grandes empresas de telecomunicaciones estadounidenses (ej: Hotmail, Yahoo, Gmail).Tanto los contenidos de esas cuentas de correo como sus datos de tráfico y los contractuales asociados, suelen estar alojados en servidores de esas empresas que, al radicar en el territorio de los EEUU, rigen su intervención o cesión conforme a su propia legislación, recogida en la *Electronic Communications Privacy Act* (ECPA) de 1986, en la que se distingue cuando se requiere o no comisión rogatoria para esa cesión:

1º) Obtención de datos directamente del ISP mediante mandamiento judicial, pedidos directamente a la empresa proveedora de servicios de correo electrónico, sin comisión rogatoria.

En algunos casos los ISP alojados en los EEUU o sus afiliados en país extranjero pueden proporcionar directamente a las autoridades extranjeras ciertas formas de asistencia sin necesidad de presentar una solicitud formal de asistencia judicial a los Estados Unidos, cuando se trate de averiguar los siguientes datos, justificando siempre la sospecha de que se tengan esos datos por parte del proveedor de servicio[384]:

- Datos de registro, teléfono, titularidad o posible cuenta alternativa.
- Posibles datos de pago o domiciliación bancaria.
- Números de conexión IP de los accesos a las bandejas de correo.
- Lista de contactos de la cuenta.
- Nombre de un espacio creado por una cuenta de correo.
- Nombre de un perfil creado por una cuenta de correo.

[383] En consecuencia, cuando sólo se conozca la cuenta de correo electrónico, es procedente preparar la futura comisión rogatoria al país que posea los datos necesarios, mediante un oficio previo transmitido urgentemente vía Interpol, solicitándole la congelación y conservación de los datos que luego se formalizará por la vía ordinaria a través de la oportuna cooperación Judicial. Fuera del caso de la Unión Europea, que en su Directiva 2006/24/CE, aunque declarada nula, establecía a sus Estados Miembros en su art 6 un plazo común de conservación para los datos de tráfico telecomunicativos de entre seis meses y dos años, el resto de países tienen plazos de conservación muy diferentes, EE.UU. sólo de 90 días, o no los tienen.

[384] SÁNCHEZ SISCART, J M. "Cibercrimen y cooperación judicial. Especial referencia a los ISP alojados en EE.UU". Revista Poder Judicial nº 91, quinta época año 2011. Foro de opinión. pág. 39.

- Nombre de grupos a los que pertenezca la cuenta de correo.
- Windows Live Records o números de conexión IP Passport.

En estos casos, que suelen coincidir con la radicación de sucursales en España (siendo paradigmático el de Microsoft)[385], las empresas proveedoras, siempre que haya mandamiento judicial español remiten al juzgado los datos de conexión y los del usuario de la cuenta de correo electrónico y contractuales asociados que se les solicita, sin necesidad de emitir comisión rogatoria.

No ocurre lo mismo respecto de la intervención del contenido del mensaje, que suele exigir la emisión de comisión rogatoria.

2º) Obtención de datos mediante solicitud de asistencia judicial, a través de la oportuna comisión rogatoria internacional. Distinguimos[386]:

A) Para obtener de un ISP que se encuentre en EEUU la divulgación de contenidos podrá dirigirse la solicitud formal de asistencia que incluya una descripción precisa de los datos que se tratan de obtener y una explicación detallada de las razones por las que la obtención de estos datos ayudaría a la investigación, pues únicamente podrá emitirse una orden del Tribunal competente para su divulgación si se ofrecen hechos específicos y claramente expresados que demuestren que existen motivos razonables para creer que el contenido o los registros, u otra información buscada son pertinentes e importantes para la investigación en curso.

Si se concede la orden de divulgación, el ISP o servicio de hospedaje de sitios web copiará los datos solicitados y los entregará en un medio electrónico o impreso en papel, o de ambas formas, a la autoridad de los Estados Unidos que ejecuta la solicitud para el país en el extranjero.

[385] Si el proveedor es MICROSOFT CORPORATION (actualmente presta los servicios Hotmail, MSN, Windows Live, y sus servidores se encuentran en EEUU) el juez Español podrá solicitar esos datos a su filial en España quién contestará directamente al Juzgado o grupo policial que haya gestionado el Mandamiento. Microsoft conserva durante 60 días las IP de acceso a las bandejas de correo electrónico y los datos de Windows live durante 365 días, pero a medida que se use la cuenta se irán sobrescribiendo.

[386] SÁNCHEZ SISCART, J. M. "Cibercrimen y cooperación judicial. Especial referencia a los ISP alojados en EE.UU (…)". ob. cit pág. 39.

En concreto será necesario cumplimentar una comisión rogatoria cuando se trate de averiguar el contenido de una cuenta de correo electrónico, el contenido de alguno de sus mensajes, de sus destinatarios, las denominaciones de los asuntos de los mensajes, las iP Log, el contenido existente en grupos, espacios, skydrive, perfiles, etc. Para conseguir esa información es preciso definir detalladamente la existencia de indicios de criminalidad suficientes (causa probable) y la concreta relación o nexo causal entre los hechos delictivos y las cuentas de correo o los concretos mensajes enviados. En caso contrario la autoridad judicial requerida puede denegar la orden de registro[387].

Por último, hay que señalar que las autoridades de EEUU no suelen otorgar prioridad a las peticiones de auxilio judicial relacionado con delitos menos graves o cuya cuantía económica no exceda de una determinada cantidad. Así, los hechos leves y medios entre los que la legislación norteamericana comprende las expresiones vejatorias a través de internet, por obra de su concepción amplia del derecho a la libertad de expresión contemplado en la Primera Enmienda a su Constitución, suelen dar lugar a la no concesión de lo solicitado.

De otra parte, hay que tener presente para la cesión de datos de tráfico, del usuario e incluso a veces de la cuenta bancaria asociada si el correo no es gratuito, que las empresas proveedoras de servicios estadounidenses sólo tienen la obligación de conservarlos por un período que oscila entre los 20 y los 60 días. Como cualquier comisión rogatoria a EEUU va a dilatar más tiempo (traducción, transmisión a través de las respectivas autoridades centrales, etc.), y con la idea de prevenir la destrucción y borrado de los datos requeridos por la empresa sin recuperación alternativa, la única vía eficaz posible consiste en emitir una "orden de conservación" del art. 588 octies de la LECrim (auto del juez requirente al requerido explicando sucintamente la vinculación y

---

[387] SÁNCHEZ SISCART, J. M. "Cibercrimen y cooperación judicial. Especial referencia a los ISP alojados en EE.UU (…)". ob. cit. pág. 41.
"La solicitud de asistencia para obtener la orden de registro, debe cumplir en la medida de lo posible lo siguiente:

1. *Debe describirse el lugar específico que se ha de registrar y los objetos específicos que deben obtenerse*.
2. *Debe aportarse información confiable que demuestre que es probable que se encuentren las pruebas del delito en el lugar que se va a registrar.*
3. *La información no puede ser demasiado antigua, pues de lo contrario, puede considerarse que ya no es probable que existan pruebas en el lugar que se va a registrar*.

necesidad de preservar el dato sin destruirlo como relevante en la investigación penal, trasladado vía Interpol, con el compromiso de solicitarlo formalmente emitiendo la correspondiente comisión rogatoria una vez conservado).

Si la "orden de conservación" es aceptada produce el efecto de hacer que los datos *ad hoc* requeridos se conserven noventa días más, que pueden prolongarse por otros noventa adicionales en caso de que lo investigado tenga la consideración de hechos graves (ej. crimen organizado, terrorismo).

B) Para la intervención del contenido de una cuenta de correo electrónico en tiempo real:

La legislación de EE.UU. no contempla, en principio, la intervención en tiempo real de un correo electrónico autorizado por la legislación de país extranjero, si con ella se trata de investigar hechos delictivos ocurridos en otro país, a menos que a la vez abra una investigación paralela por el mismo objeto.

Si se acuerda no investigar, la cooperación judicial penal estadounidense consiste en la aportación del barrido histórico de los mensajes enviados y recibidos en un determinado período de tiempo, sin que se pueda conocer su contenido.

En caso contrario, la justicia norteamericana exige comisión rogatoria y mandamiento *(warrant)* del juez estadounidense, por lo que los datos consignados en la comisión rogatoria deben ser exhaustivos por parte del juez requirente para superar la llamada *"probable cause"* o juicio suficiente de probabilidad o ponderación. Para ello, se necesita informar suficientemente de los indicios delictivos detectados, su relación probatoria probable con el correo electrónico a intervenir y la copia de los preceptos del Código Penal español infringidos, que llevarán o no al juez norteamericano a emitir la orden permitiendo o no la intervención de la cuenta de correo electrónico que, como decimos, además, deberá haber propiciado una investigación paralela sobre los mismos hechos en su territorio.

Por otra parte, el alcance del contenido de la injerencia judicial que supone la intervención del correo electrónico abarca además del mensaje de texto, todos sus anexos conteniendo a su vez texto, imagen o voz, y los datos de tráfico vinculados a los

mismos y que se transmitan con estos (en poder de la empresa de telecomunicación y en su cabecera técnica) y los datos contractuales derivados de la concertación del servicio.

b) SMS y MMS.

El *Short Message System* (SMS), que trasmite mensajes por escrito telefónicamente, al igual que el *Multimedia Messaging System* (MMS), que trasmite imágenes entre teléfonos móviles, se encuentran encuadrados en el concepto de correo electrónico y que recoge el art. 2 h) de la Directiva CE 58/2002, de 12 de julio.

Su consideración como verdaderos correos electrónicos les hace extensibles a las consideraciones jurídicas ya señaladas para el *e-mail*: es decir, son auténticas telecomunicaciones para cuya intervención, es necesaria la preceptiva autorización judicial, igual que para la ocupación de su contenido almacenado (después de recibido y leído o cuando esté almacenado para ser emitido o para ser leído) dada la protección formal del mismo salvo razones de estricta y necesaria urgencia, en que la validación judicial se hará a *posteriori*[388].

La valoración judicial para autorizar su injerencia debe ser en todo caso ex *ante,* y no podrá determinarse en función del contenido hallado después. Al no tratarse de correo epistolar ni postal (pues el envío del mensaje no se paraliza sino que se monitoriza, y su transmisión es electrónica o magnética) le son aplicables las disposiciones que regulan la intervención telefónica en los párrafos 588 ter, y 188 de la LPM, y no las que recogen los arts. 579 LECrim y 187 LPM.

Desaparecido el proceso comunicativo, y a diferencia de lo que suele ocurrir con las conversaciones orales telefónicas, el mensaje en el SMS y MMS se conserva, por lo que su ocupación en el terminal emisor o receptor, continúa protegida por el derecho,

[388] Y en similares términos a lo hasta ahora expuesto respecto de los *e-mails*, puede darse por referido a los mensajes cortos de texto de teléfonos GSM o de PDA's, en donde se precisa la autorización judicial para poder proceder al análisis de los archivos de fotos o de mensajes msm de un teléfono móvil interceptado del presunto autor de un delito.

esta vez a la intimidad, para cuya afectación también es necesaria la obligada autorización judicial[389].

c) Mensajería Instantánea y las comunicaciones VoIP.

La mensajería instantánea *(instant messaging)* difiere del correo electrónico en que las conversaciones son en tiempo real (Skype, Line, Telegram…). Las comunicaciones mediante el tráfico de voz sobre IP *(VoIP),* se trata de una conversación entre dos interlocutores, cada uno de ellos desde su teléfono, sin que estemos en absoluto ante una "comunicación telefónica". El ejemplo paradigmático es el *"WhatsApp"* que es una aplicación de mensajería multiplataforma de gran arraigo que permite enviar y recibir mensajes y efectuar llamadas *VoIP* .

WhatsApp utiliza el plan de datos de los teléfonos móviles. La información que se envía a través de este servicio se almacena en los servidores de WhastsApp, que están localizados en el Estado de California (EEUU). Los usuarios son advertidos de que su uso lleva implícito la aceptación de la política de privacidad y las condiciones del servicio, que están bajo las leyes del Estado de California y que toda la información que se trasmita mediante el servicio de WhatsApp es transferida a los EEUU, y por tanto muestran su consentimiento a que sean amparadas bajo las leyes de del Estado de California.

Cuando se utiliza WhatsApps los servidores del mismo registran automáticamente, la siguiente información[390]:

[389] STS 884/2012 de 8 noviembre. "No puede existir duda alguna acerca de la catalogación del mensaje SMS como correo electrónico. Es cierto que no todos los contenidos imaginables de mensajería mediante teléfono móvil pueden aspirar al mismo grado de protección constitucional. No faltan casos en que el SMS se utiliza con una finalidad distinta a la transmisión de un pensamiento o de una imagen. Pensemos en su extendida utilización como forma de aviso, de comunicación, de participación en concursos, como receptor de alarmas o de titulares de un medio de comunicación. Pero lo que no es cuestionable -más allá de los matices que podrían hacerse en función del momento en el que se produce la injerencia, si ésta tiene lugar cuando el texto ya ha sido leído y simplemente está archivado- es que el mensaje de texto (Short Message System) entra de lleno en el contenido de la inviolabilidad de las comunicaciones. También participa de la misma naturaleza el MMS (Multimedia Messaging System), esto es, el mecanismo técnico que permite el envío de imágenes entre teléfonos móviles.

- La petición web.
- La dirección IP.
- La versión del sistema operativo (android, Apple iOS)
- El idioma utilizado.
- El tipo de plataforma desde el que se accede al servicio.
- Nombre de dominio del que se accede al servicio.
- El número de mensajes.
- Fecha y hora de cada mensaje.
- Número de teléfono origen del mensaje.
- Número de teléfono destino del mensaje.

WhatsApp no registra nombres, direcciones de correo u otra información de contacto de las listas de los dispositivos, ni el contenido de los mensajes. Tampoco registra los datos de localización de los dispositivos, a menos que los usuarios quieran compartir voluntariamente su localización con otros usuarios utilizando el servicio de WhatsApp.

Antes de la implementación en Whatsapp del cifrado E2EE (end-to-end), el contenido de los mensajes, no eran copiados ni almacenados por WhatsApp salvo, mandamiento judicial de un Tribunal de los EEUU. El contenido del mensaje no entregado se almacenaba en los servidores de WhatsApp por un plazo de 30 días, trascurrido el mismo, el mensaje se eliminaba. El contenido solo se guardaba en los dispositivos del emisor y del receptor.[391]

Desde que se ha activado el cifrado E2EE (end-to-end)[392], que se conoce como un "protocolo severo", sólo el emisor y el receptor pueden leer los mensajes, no pueden

[390] DELGADO MARTÍN, J. "La prueba del whatsapp". Diario La Ley nº 8605, 2015. pág. 1

[391] www. WhatsApp.com/Legal.

[392] El cifrado *end-to-end* tiene como base un protocolo de señal, diseñado por Open Whisper Systems, y que impide que terceros accedan a los mensajes, documentos y llamadas. Según este protocolo, cada usuario de Whatsapp posee una clave privada de encriptado, que se crea al instalarse la aplicación y se queda en el teléfono, pero que ni siquiera Whatsapp tiene acceso a ella.
Cuando el emisor envía un mensaje a este usuario, los servidores de la aplicación utilizan una clave pública que usa para cifrar el mensaje que va a enviar y que se cambia periódicamente. Así, sólo el receptor puede leer el mensaje gracias a esa clave privada que se encuentra en su teléfono. El candado sería la clave que cifra el mensaje y la llave para abrirlo la clave privada que posee el receptor. Además, la clave cambia con cada mensaje, pues gira sobre una base temporizada.

acceder a ellos ni siquiera los proveedores de telecomunicaciones, los proveedores de internet o los dueños de la aplicación. Esto quiere decir que la compañía no tiene ninguna capacidad para acceder a los mensajes de sus clientes, ni siquiera por orden de las autoridades. *Whatsapp* no mantiene los registros de los mensajes en sus servidores una vez han sido enviados y recibidos. Lo mismo sucede con las llamadas de *Whatsapp*, cualquier llamada realizada con la aplicación, incluyendo si es al extranjero, está cifrada de extremo a extremo para que ningún tercero pueda escucharla y no puedan ser intervenidas de ninguna manera, ya que ni la aplicación, ni el servidor ni el proveedor de datos conoce la clave de cifrado, que es creada por el propio dispositivo.

Por ello, ante el uso de estas nuevas técnicas de encriptación[393], será necesario acudir a otras sofisticadas medidas de investigación tecnológica[394], como pudiera ser el registro remoto de equipos informáticos, para acceder al contenido forma remota mediante la introducción de un malware en el equipo a intervenir, sin que sea necesario así solicitar la colaboración del ISP.

d) Redes Sociales.

En primer lugar, conviene destacar que estas empresas dedicadas a la introducción de contenidos en internet no los pueden controlar (pues técnicamente solo son intermediarios de la circulación de información), y sería exacerbado imponerles su vigilancia. Se les ha exigido (art. 11 de la Ley *34/2002,* de 11 de julio, de servicios de la Sociedad de la información y de comercio electrónico) un carácter de *custodia pasiva*[395]*,* de modo que responderán penalmente, en su caso, no por no haber detectado en sus páginas la existencia de contenidos ilícitos, sino si una vez hecho, notificado,

[393] También usadas por otras aplicaciones como Telegram que permite la autodestrucción del mesaje.

[394]En el caso Diana Quer la Policía para poder visualizar los mensajes de whatsApp solicitó un clonado de la tarjeta SIM la introdujo en un equipo y puso en marcha WhatsApp. Gracias a ello pudieron visualizar los mensajes recibidos por Diana que no llegó a ver, pese a que no pudieron entrar a los destinados por ella o a los que ya había leído.

[395] Arts. 13 a 17 de la Ley 34/2002, de 11 de julio, de servicios de la Sociedad de la información y de comercio electrónico. "*Sobre el Régimen de Responsabilidad"*

ordenado o sabido, éstos no los retiran (comisión por omisión), además de en los supuestos en que ellos sean los propios creadores directos o cooperadores necesarios en la difusión del contenido ilícito o asuman el papel de moderadores o gestores responsables, por ejemplo de foros de debate[396].

Algunas de las manifestaciones más frecuentes son:

- Los chats: del inglés *"chat"* (charla), es un sistema de mensajería instantánea dentro de una red social. Es una conversación dialogada por escrito que puede llegar a ser en tiempo real entre varias personas, pero transmitida por la misma vía electrónica o magnética que el correo electrónico, ya que en realidad se trata de correos electrónicos encadenados y en tiempo real. El chat puede ser abierto o cerrado, según se conozca y permita participar libre o restringidamente en la conversación, y suele ser de un emisor a múltiples receptores, no exigiendo identificación verdadera de los comunicantes (al revés, suele hacerse con participantes que tan sólo se identifican a través de los correspondientes *nicks,* apodos o pseudónimos), residiendo la información sobre el mismo en el servidor del chat (a cuya empresa servidora habrá que solicitársela) y no en los ordenadores desde los que se participa en el chat.

Desde un punto de vista jurídico, los chats abiertos no plantean problemas de injerencia en derechos fundamentales por lo que para conocer su desarrollo y ocupar su contenido, basta con la realización de la oportuna inspección ocular directa y su introducción al proceso por cualquier medio que deje constancia de su fehaciencia en el mismo (documental con fe del LAJ, testifical, etc.). Paradójicamente, para la consecución de los datos de tráfico de los participantes, el criterio no debiera ser el contrario, sino lógicamente el mismo (quien puede lo más, puede lo menos), por no estar los datos de tráfico del chat protegidos por el derecho al secreto de las comunicaciones, si bien se requiere autorización judicial por ser datos almacenados en operadoras a los que se refiere la ley 25/2007 que requieren del procedimiento de cesión previsto en LECrim.

Más problemática es la consideración jurídica sobre la naturaleza de las comunicaciones en los chats cerrados. Al caracterizarse por su deseo formal de excluir

[396] AGUSTINOY GUILAYN, A Y MONCLÚS RUIZ, J. "Aspectos legales de las redes sociales". Colección Práctica Jurídica. Ed. Bosch, Barcelona, 2016.

de su conocimiento y participación a terceros ajenos no autorizados, sí se incide en el derecho al secreto de las comunicaciones lo que exige la necesaria autorización judicial para su investigación.

- Foros: a diferencia del chat, el foro suele tener un marcado carácter de permanencia y se suele vincular a un colectivo o tema concreto. Por ello, su función no suele ser tanto la conversación, cuanto dar o proporcionar información sobre un colectivo o tema monográfico. La naturaleza de la intención -más o menos divulgativa- del foro puede ser la clave para entender si se está ante un foro público abierto o un foro reservado o privado, de cara a considerar si las comunicaciones e información obrantes en el mismo deben o no tener la protección jurídica reforzada que acabamos de analizar para los chats abiertos o cerrados. Obviamente, la información sobre el mismo se aloja en el servidor del foro y no en el PC de los usuarios, y es de la empresa servidora a la que debe recabarse.

- Blogs: los *blogs* o "diarios en la Red"comportan un carácter mixto entre una web y un *log,* constituyéndose en páginas informáticas abiertas al conocimiento público, que además de actualizarse periódicamente suelen contar con anotaciones personales de su responsable, pero al tener ese carácter público deben tener la protección jurídica que acabamos de analizar para los chats abiertos.

- Facebook, Twitter, Youtube: como información relevante de cara a la investigación criminal, hay que saber que este tipo de redes sociales almacena una información de registro en la misma, que incluye: nombre, dirección de correo electrónico, fecha de nacimiento y sexo, y en algunos casos un número de teléfono. Además de esta información, que puede ser falsa pues no se comprueba su autenticidad, cada vez que se interactúa en la red social, los servidores almacenan información del ordenador, teléfono móvil o dispositivo que se utiliza, la dirección IP desde la que se accede, el proveedor de servicio de internet, la ubicación, y el tipo de navegador. En

algunos casos determinadas redes sociales almacenan las coordenadas GPS u otros datos de ubicación[397].

Estas redes sociales tienen su sede en EEUU, y pueden acceder a la información de tráfico y contenido, conservarla y compartirla en repuesta a una petición judicial, bajo el criterio de buena fe, que la legislación que realiza la petición les ofrece. Esta política supone respetar los requerimientos legales de jurisdicciones ajenas a los EEUU cuando crean de buena fe que las leyes locales de tal jurisdicción exigen dicha respuesta, afectan a usuarios de dicha jurisdicción y resulta coherente con estándares internacionales generalmente aceptados. También pueden acceder, conservar y compartir información cuando crean de buena fe que es necesario para detectar, prevenir y abordar, actividades fraudulentas o ilegales; para proteger sus propios servicios o a sus usuarios, incluso como parte de investigaciones, y para evitar muertes o daños físicos inminentes.

Por otra parte, estas redes sociales manifiestan en sus políticas de uso de datos que podrán consultar, procesar o conservar la información de los usuarios incluida información sobre transacciones financieras relativas a compras realizadas en estas redes durante un periodo prolongado de tiempo, cuando esté sujeta a una solicitud u obligación judicial, una investigación gubernamental o investigaciones relacionadas con posibles infracciones de las políticas o condiciones de uso del servicio o bien para evitar daños. Por último, estas redes conservan la información de las cuentas que se han desactivado por incumplimiento de las condiciones de uso durante un año[398].

[397] www. Facebook.com/full_data_use_policy.

[398] STS 106/2015 de 19 de febrero. *"(...)importancia de las redes sociales tiene su incidencia en el sistema penal, cualquier política criminal hoy día no puede ignorar esta explosión tecnológica que permite divulgar cualquier mensaje en pocos segundos a una multitud de usuarios situados en países lejanos con lo que se obtiene una publicidad de los mensajes impensable hace unos años*." Referido a delito de enaltecimiento del terrorismo a través videos subidos en youtube. En el mismo sentido la STS 623/2016 de 13 julio, la comisión del delito de enaltecimiento del terrorismo a través de twiter no requieren que el sujeto activo del mismo sea el inventor de las proclamas, mensajes, comentarios, etc. a través de los cuales se perpetran el ilícito penal. El hecho de publicitarlos en su cuenta TWITER logrando así su difusión entre sus seguidores, colman las exigencias típicas de naturaleza objetiva contenidas en el artículo 578 del Código Penal. Lo mismo la STS 820/2016, de 2 de noviembre sobre delito de odio a través de Facebook.

2)Terminales objeto de intervención.

a) Identificación del terminal.

La identificación del terminal o terminales objeto de injerencia ha pasado a ser un componente esencial de cualquier título habilitante; su omisión, como advierte la STS 201/2006, de 1 de marzo, podría dar lugar a la apreciación de un vicio en el título de raigambre constitucional, con potencialidad de extender su fuerza anulatoria a todas las pruebas directas y derivadas relacionadas con la información obtenida del contenido de las comunicaciones interceptadas[399].

Desde el ángulo opuesto, se admite también la fijación del objeto de la intervención por la identidad de la persona investigada (STS 1046/2002, de 3 de junio)[400]. El Tribunal Supremo justifica la proporcionalidad de la medida así acordada

[399] Debe, pues, determinarse con precisión el número o números de teléfono que han de ser intervenidos (SSTC 26/2010, de 27 de octubre; 259/2005, de 24 de octubre; 136/2006, de 8 de mayo).
Es frecuente la alegación de que la policía no indicó cómo obtuvo el número de teléfono. Esta alegación carece de trascendencia. En este sentido pueden citarse las SSTS 1161/2011, de 31 de octubre, 1078/2011, de 24 de octubre y la 940/2011, de 27 de septiembre. Es también frecuente que se alegue ilegitimidad en el procedimiento empelado por la Policía para identificar el número telefónico del sospechoso, sin aportar ningún indicio de ilegitimidad. Tal alegación debe ser rechazada sin mas, existiendo una copiosa doctrina de nuestros tribunales en el sentido de que no es exigible que la Policía acredite no haber infringido derechos fundamentales salvo que se ofrezcan indicios de ilegitimidad en la obtención de la información. No es admisible extender una presunción de ilegitimidad a toda actividad policial (SSTS 85/2011 de 7 de febrero, 1003/2011 de 4 de octubre, 509/2009 de 13 de mayo; 309/2010, de 31 de marzo). No es preciso acreditar la forma de obtención del número de teléfono de un sospechoso cuando no hay indicios de ilegitimidad en el proceso de obtención de la información, ya que es exigible a los poderes públicos que justifiquen que la restricción de un derecho fundamental se ha realizado con respeto a las reglas, pero no lo es que demuestren que no lo han hecho (SSTS 207/2012, de 12 de marzo; 509/2009, de 13 de mayo; 309/2010, de 31 de marzo; y 862/2010, de 4 de octubre). La validez constitucional de las escuchas no depende de la constancia documentada de los términos en los que fueron obtenidos los números de teléfonos sujetos a observación (STS 751/2012, de 28 de septiembre). La STC 25/2011 de 14 de marzo declara, además que en todo caso la vulneración del derecho a la intimidad al obtener la titularidad y el número del teléfono móvil sería una injerencia en la intimidad de carácter leve "que, con arreglo a nuestro canon constitucional podría considerarse proporcionada al constituir un medio idóneo para un fin legítimo"

[400] El TS admite la intervención en supuestos en los que el único dato fiable para la identificación personal del sujeto investigado no va más allá de su sobrenombre, o determinados rasgos físicos (STS 832/2001, de 14 de mayo) o el lugar donde reside, con o sin identificación del propietario de la vivienda donde se encuentra ubicado el terminal de telefonía fija (SSTS 606/1994, de 18 de marzo; 768/1995, de 14 de junio, y 1052/1998, de 21 de septiembre).
Tampoco ha de considerarse en todo caso relevante el error sobre el titular del teléfono o el usuario del mismo cuando la línea telefónica intervenida resulta correctamente identificada (STC 220/2009, de 21 de

con el argumento de la necesidad de dar una respuesta ágil a los continuos cambios de número que los abonados realizaban, que en ningún momento implica indeterminación de la línea realmente intervenida.

Se han planteado dudas acerca de la necesidad de identificar plenamente a la persona antes de proceder a intervenir sus comunicaciones. La jurisprudencia se ha pronunciado en contra de esta exigencia, señalando la STS 309/2010, de 31 de marzo que "*el hecho de que no se aporten otros datos de identidad no puede ser, en modo alguno, obstáculo para la legitimidad de la interceptación"*. Así lo ha declarado en ocasiones precedentes, la jurisprudencia del Tribunal Constitucional, de la que la Sentencia 150/2006, 22 de mayo, es elocuente ejemplo: "*... más allá de ello, y aunque en varias sentencias se ha hecho referencia, como expresión del alcance subjetivo de la medida, a la importancia de identificar las concretas personas investigadas como usuarias del teléfono intervenido (entre las últimas, SSTC 171/1999, de 27 de septiembre, F. 7; 138/2001, de 18 de junio, F. 5 ó 184/2003, de 23 de octubre, F. 10), del conjunto de la jurisprudencia de este Tribunal, construida fundamentalmente para dar respuesta a casos en que se plantean otro tipo de problemas, no se desprende que la previa identificación de los titulares o usuarios de las líneas telefónicas a intervenir resulte imprescindible para entender expresado el alcance subjetivo de la medida,*

---

diciembre y STS 1151/2010, de 17 de diciembre). No tiene más trascendencia la simple confusión en la identificación nominal del usuario (SSTC 104/2006, de 3 de abril, y 150/2006, de 22 de mayo). El ATC 245/2007, de 22 de mayo considera que si bien es cierto que en determinadas sentencias se ha resaltado la importancia de identificar a las concretas personas investigadas como usuarias del teléfono objeto de la intervención…apreciando globalmente la doctrina constitucional se desprende que no puede otorgarse relevancia constitucional a cualquier error en la identidad de los titulares o usuarios de las líneas a intervenir. El auto analiza un supuesto en el que tras una inicial indefinición, no acerca de la persona afectada por la medida, sino sobre sus concretos datos identificadores, aparecían con precisión los hechos investigados y se especificaba el usuario del teléfono intervenido. Para el TC no cabe hacer reproche constitucional puesto que no existió equivocación alguna acerca de la persona sobre la que se centraban las investigaciones, sino exclusivamente sobre su nombre, y concurrió por tanto la necesaria conexión entre el delito investigado y el destinatario de la medida. La STC 104/2006, de 3 de abril considera irrelevante el error en el nombre del usuario valorando especialmente que "sólo hubo una línea de teléfono móvil intervenida, identificada en la resolución judicial de autorización por el único dato fiable existente en ese momento -su número-, dada la modalidad prepago de la tarjeta con la que funcionaba".

La STC 150/2006, de 22 de mayo declara, partiendo de los avances tecnológicos en el campo de la telefonía, que tan solo será constitucionalmente exigible la aportación de los datos que resulten imprescindibles para verificar la idoneidad y rigurosa necesidad de la medida, debiendo apreciarse la suficiencia o no de los datos aportados en relación con las circunstancias concretas que concurran en el momento de autorizar la intervención.

El hecho de que la autorización se otorgue para identificar a otras personas implicadas no supone una indeterminación subjetiva que ponga en cuestión la legitimidad de la medida (ATC 35/2010, de 9 de marzo).

excluyendo la legitimidad constitucional de las intervenciones telefónicas que, recayendo sobre sospechosos, se orienten a la identificación de los mismos u otorgando relevancia constitucional a cualquier error respecto de la identidad de los titulares o usuarios de las líneas a intervenir. A la vista de los avances tecnológicos en el ámbito de la telefonía -por ejemplo, con la aparición de teléfonos móviles y tarjetas prepago, que dificultan la identificación de los titulares y usuarios, facilitando el intercambio de los teléfonos, esas exigencias resultarían desproporcionadas por innecesarias para la plena garantía del derecho y gravemente perturbadoras para la investigación de delitos graves, especialmente cuando éstos se cometen en el seno de estructuras delictivas organizadas ".

En el caso de utilización de tarjetas prepago el único medio de identificación pueden ser los números, y ello debe entenderse perfectamente admisible. La STC 104/2006, de 3 de abril permite la identificación de la persona concernida solamente por el único dato conocido hasta el momento, el número de abonado de terminal de telefonía móvil[401]. Debe en este punto recordarse que la Disposición Adicional Única de la Ley 25/2007, de 18 de octubre impone a las operadoras la obligación de la llevanza de un registro en el que conste la identidad de los clientes que adquieran una tarjeta de telefonía móvil mediante la modalidad de prepago y que las operadoras deben ceder los datos en el período durante el que es obligatoria su conservación a los miembros de las Fuerzas y Cuerpos de Seguridad del Estado y de los Cuerpos Policiales de las Comunidades Autónomas con competencia para la protección de las personas y bienes y para el mantenimiento de la seguridad pública, o al personal del Centro Nacional de Inteligencia, así como a los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, cuando les sean requeridos por éstos con fines de investigación, detección y enjuiciamiento de delitos.

Tampoco el defecto consistente en la errónea identificación del usuario del teléfono intervenido afecta a la validez de la medida ni al derecho fundamental al secreto de las comunicaciones, ya que como señala la STS 2026/2001, de 28 de noviembre, "*en todo caso el teléfono realmente intervenido pertenecía a un sospechoso, por lo que la medida judicial estaba suficientemente justificada. Todas las*

[401] Las SSTC 104/2006, de 3 de abril, 150/2006, de 22 de mayo, así como la STS 2026/2001, de 24 de octubre, admiten la identificación tan sólo por el número de terminal, en un momento de la investigación en el que la identidad del titular o usuario descubierto era un dato inexistente o poco fiable.

conversaciones que pasaban a través del teléfono realmente intervenido, eran de incuestionable interés para el curso de las investigaciones, por lo que todos los interlocutores podían ser grabados sin que por ello se resintiesen sus derechos fundamentales al secreto de las comunicaciones". En los mismos términos, la STC 150/2006, de 22 de mayo, señala que "*del conjunto de la jurisprudencia de este Tribunal, construida fundamentalmente para dar respuesta a casos en que se plantean otro tipo de problemas, no se desprende que la previa identificación de los titulares o usuarios de las líneas telefónicas a intervenir resulte imprescindible para entender expresado el alcance subjetivo de la medida, excluyendo la legitimidad constitucional de las intervenciones telefónicas que, recayendo sobre sospechosos, se orienten a la identificación de los mismos u otorgando relevancia constitucional a cualquier error respecto de la identidad de los titulares o usuarios de las líneas a intervenir"*.

La reforma de la LECrim operada por Ley Orgánica 13/2015, de 5 de octubre, recoge esta doctrina jurisprudencial al señalar entre los requisitos que debe reunir la solicitud de intervención de las comunicaciones (artículo 588 bis b 2.1º), la identidad del investigado siempre que este dato resulte conocido, con lo que admite *a sensu contrario* la posibilidad de intervención en los supuestos en los que dicho dato no resulte conocido.

b) Titularidad del terminal.

La persona investigada no tiene que ser necesariamente titular del terminal objeto de injerencia[402]. La intervención podrá afectar a los terminales o los medios de comunicación de los que el investigado sea titular o usuario, pero también si pertenecen a una tercera persona, en los tres casos previstos en el artículo *588 ter c* de la LECrim*:*

1. Que exista constancia de que el sujeto investigado se sirve de aquélla para transmitir o recibir información.

[402] (SSTS 1154/2005, de 17 de octubre; 463/2005, de 13 de abril).

Se podrán intervenir terminales o medios de comunicación de los que sean titulares personas distintas de las investigadas, cuando existan fundadas sospechas de que los investigados utilicen teléfonos de familiares o allegados precisamente para intentar esquivar posibles intervenciones[403].

2. Que el titular colabore con la persona investigada en sus fines ilícitos o se beneficie de su actividad. En este caso dicho tercero se convierte técnicamente en cómplice o cooperador necesario.

3. Cuando el dispositivo objeto de investigación sea utilizado maliciosamente por terceros por vía telemática, sin conocimiento de su titular.

Este último caso hace referencia implícita a los sistemas de infestación de terminales tales como los troyanos, que permiten visualizar e incluso manejar un terminal telemáticamente[404].

Esta expresa previsión legal pone fin a las dudas que estos supuestos habían generado anteriormente, asumiéndo la interpretación seguida por el Tribunal Supremo (*vid.* STS 23/2007, de 23 de enero y STS 745/2010, de 26 de julio).

Con esta regulación queda claro que no es necesario que el terminal esté a nombre o sea propiedad del investigado, cuestión ésta cuya indeterminación había generado dudas. La STS 84/2010, de 18 de febrero aclaró que en caso de que el sujeto investigado emplee un teléfono del que no es titular, la autorización judicial concedida puede estar justificada por el hecho del uso, no siendo atendible la alegación por parte del investigado de la supuesta lesión de derecho perteneciente al titular cuando, con respecto a éste, no se haya autorizado la observación. En este caso deberá extremarse la motivación, ya que se afecta, al mismo tiempo, al derecho a la intimidad y secreto de las comunicaciones de personas que, en principio, no están directamente implicadas en las investigaciones en marcha (STS 960/1999, de 15 de junio).

[403] Para la STS 606/1994, de 18 de marzo "obvio resulta…la posibilidad de intervención de teléfono de persona no imputada, ni ,en principio, objeto de sospecha de una intervención directa, cuando tal teléfono es el que utiliza o del que se sirve el sujeto sobre el que existen indicios de actuación criminal, para la mejor planificación y desarrollo de sus propósitos delictivos". En el mismo sentido, SSTS 463/2005, de 13 de abril y 543/2002, de 25 de marzo.

[404] GIMENO BEVIÁ, J. "Análisis crítico de la reforma de la LECrim 2015 (…)". ob. cit. pág. 9

También podrán intervenirse *los terminales o medios de comunicación de la víctima cuando sea previsible un grave riesgo para su vida o integridad* (art. 588 ter b LECrim).

Por otra parte, es admisible acordar la intervención sobre terminales públicos, adoptando medidas para evitar la intromisión en comunicaciones de personas ajenas a la investigación[405].

Singular interés plantea la intervención de comunicaciones realizadas en *cibercafés, locutorios* y *lugares públicos lucrativos* o no, de emisión y recepción de telecomunicaciones. En principio, como los cibercafés son establecimientos públicos no sería necesario el mandamiento judicial para su entrada y registro, salvo que se pretenda realizarlo en zonas donde, dentro de él, se desarrolle vida privada (reservados, despachos, etc.).

Por el contrario, las comunicaciones que los usuarios realizan en ellos son siempre privadas. Esto supone que para la interceptación e intervención de su contenido, siempre será necesario mandamiento judicial otorgado en el curso de una investigación judicial abierta, y que por lo tanto no puede ser prospectiva.

Cualquier observación realizada desde el ordendador de un cibercafé sin mandamiento judicial para ver lo que se transmite desde otro ordenador supondría una vulneración del derecho al secreto de las comunicaciones del espiado por lo que la información así obtenida podría ser nula jurídicamente[406].

---

[405] La STS 467/1998, de 3 abril declara al respecto que carece de fundamento la objeción de haberse pinchado un teléfono público, dado que era precisamente el mismo el utilizado por los acusados y a cuyo través adoptaban acuerdos y formulaban instrucciones….lo cierto es que la Juez de Instrucción fue sumamente cautelosa al respecto, cual exigían las propias connotaciones de la línea a interceptar, ordenando que en la medida de lo posible, la observación no alcanzara a personas no sometidas a investigación. Y a ello atendió la fuerza instructora del atestado, efectuando periódicas y discretas vigilancias por los alrededores del bar y avisando mediante equipos portátiles a sus compañeros cuando los investigados entraban en el establecimiento, en orden a que prestaran atención a la eventual conversación que pudiera producirse de forma inminente. Bien resulta el exquisito control judicial eliminando las conversaciones de aquellas personas a quienes no afectaba el auto de intervención. En la misma línea, *vid*. STS 787/1994, de 18 de abril.

[406] VELASCO NÚÑEZ, E. "Delitos cometidos a través de Internet (...)". ob. cit. págs. 109 y 110.
En ese sentido, la SAP Asturias Sección 3.3 de 29 de noviembre de 2004 establece que observar las comunicaciones ajenas es una facultad que sólo corresponde al instructor judicial en el marco de un procedimiento penal abierto y que, por ello, se vulnera el derecho al secreto de las comunicaciones y constituye prueba prohibida la conseguida por detectives privados que, siguiendo al sospechoso hasta un

Por último, señalar que es posible la intervención de las comunicaciones en relación con un terminal sustraído. Debe partirse del dato técnico de que pueden intervenirse las comunicaciones de origen o de destino de un terminal sustraído a través de su identificación en la red por su correspondiente número IMEI. De este modo pueden localizarse cualesquiera tarjetas SIM que se puedan insertar en el chasis para identificar a los ilegítimos usuarios[407].

---

cibercafé, se sitúan en el ordenador contiguo y, mirando por encima del hombro lo que escribía en su pantalla el investigado, observan el nombre de usuario, el del destinatario y cómo envía cierta cantidad de correos electrónicos de contenido injurioso contra personas de la empresa en la que él resultó ser sindicalista. Según esta teoría, el acceso por la vía descrita a datos que identifican al autor de la remisión de los correos electrónicos injuriosos, "se encuentra protegido por el secreto a las comunicaciones, y llevada a efecto en la forma reseñada, sustrayendo la intervención judicial, implica una obtención inconstitucional de la prueba pretendida", pues "el concepto de secreto que aparece protegido en el art. 18.3 CE, no cubre sólo el contenido de la comunicación, sino también, en su caso, otros aspectos de la misma, como, por ejemplo, la identidad subjetiva de los interlocutores o de los corresponsales" y cita en su apoyo la STEDH 2/08/1984, caso *Malone,* que considera violado el art.8 CEDH por el uso de la técnica *"comptage",* que es el empleo de un artificio *técnico* que permite registrar cuáles han sido los números telefónicos marcados sobre un determinado aparato, sin conocimiento del contenido de las conversaciones efectuadas -lo que se dice un auténtico mero dato de tráfico-.
Sin embargo, no sólo por la antigüedad y el contexto en que se dictó tal sentencia, sino por su fondo también, no se puede compartir el criterio indicado -muy discutible- en cualquier contexto comunicativo, por cuanto la identidad del comunicante hecha en lugares públicos como cibercafés no es un dato protegido -que se consigue mediante la testifical del autor de las vigilancias-, mientras que sí lo es el contenido en sí mismo, y la prueba evidente es que basta con mirar por encima del hombro -algo que ni es subrepticio, ni sofisticado ni injerente, pues no necesita de la intermediación de ningún instrumento distinto a la vista, propiamente dicha para saber la identidad subjetiva del autor de la comunicación, que bien pudo entrar a valorarse como prueba testifical no prohibida en el caso de autos, ya que la protección del derecho a la intimidad debe valorarse en cada caso concreto en función de la efectiva y objetiva protección que su titular da a la reserva de los extremos de su comunicación y al contenido de la misma.
De lo contrario, en los seguimientos policiales en que se revela con quién se comunica oralmente una persona vigilada cuando lo hace en lugares públicos, constituiría la prueba prohibida que no se comparte en los casos de observación de la identidad subjetiva de los comunicantes, cuando las comunicaciones ocurren en espacios no privados y, como en el caso, no son la fuente de la información afectada.

[407] Analiza un supuesto de este tipo la STS 745/2010, de 26 de julio: "*en el curso de los acontecimientos se produce la sustracción de un teléfono móvil que hacía previsible que se pudiera utilizar extrayendo la tarjeta original y sustituyéndola por otra…En esta tesitura, lo lógico es que se ordene la interceptación del teléfono a partir del IMEI, que lo identifica y constituye su seña de identidad inmodificable. A partir de este dato, es evidente que el Juez Instructor…no puede adivinar cuáles son las posibles y futuras tarjetas que se podrán insertar en el chasis, por lo que la medida de intervenir el teléfono asociado a un IMEI es perfectamente lógica…Los recurrentes no pueden pretender que se haya vulnerado su derecho al secreto de las comunicaciones al adoptar esta medida…El auto, cuya validez se impugna, resulta impecable desde el punto de vista constitucional. Especifica, de forma inequívoca, el teléfono móvil y su número original, y añade que la compañía telefónica debe facilitar todos los datos asociados a dicha línea, cuya escucha, por un plazo de treinta días, se llevará a cabo por funcionarios de la entidad que deberán también detectar todos los números de teléfono que se sirvan de forma irregular del móvil sustraído, quedando amparadas por la autorización judicial".*
La STS 23/2007, de 23 de enero también analiza un supuesto en el que se solicitaron los listados telefónicos en relación a teléfonos sustraídos y en base a documentación aportada por las propias víctimas, titulares legítimos de los mismos, quienes, por tanto dieron su consentimiento a la medida y todo ello con referencia a los números IMEI correspondientes a los teléfonos móviles sustraídos.

3) Revelación por un comunicante.

El derecho fundamental al secreto de las comunicaciones que consagra el artículo 18.3 de la Constitución Española descansa, fundamentalmente, en la protección de ese secreto frente a terceras personas extrañas a la comunicación. En consecuencia, quienes participan en la comunicación, no se ven afectados por la limitación constitucional, de manera que pueden disponer libremente del contenido de esa comunicación sin afectar al derecho fundamental. Al respecto, señala la STS 239/2010, de 24 de marzo que "*es reiterada jurisprudencia del TC, seguida por el TS e iniciada por la sentencia del TC núm. 114/1984 de 29 de noviembre*[408]*, la que establece que el derecho al secreto de las comunicaciones salvo resolución judicial no puede oponerse, sin quebrar su sentido constitucional, frente a quien tomó parte en la comunicación misma así protegida. [...] Sea cual sea el ámbito objetivo del concepto de "comunicación", la norma constitucional se dirige inequívocamente a garantizar su impenetrabilidad por terceros (públicos o privados: el derecho posee eficacia "erga omnes") ajenos a la comunicación misma. [...] No hay "secreto" para aquél a quien la comunicación se dirige, ni implica contravención de lo dispuesto en el art. 18.3 CE la retención, por cualquier medio, del contenido del mensaje. [...] Quien entrega a otro la carta recibida o quien emplea durante su conversación telefónica un aparato amplificador de la voz que permite captar aquella conversación a otras personas presentes no está violando el secreto de las comunicaciones, sin perjuicio de que estas mismas conductas, en el caso de que lo así transmitido a otros entrase en la esfera "íntima" del interlocutor, pudiesen constituir atentados al derecho garantizado en el art. 18.1 CE".*

Por otra parte, las grabación de las conversaciones por uno de los interlocutores no afectan al secreto de las comunicaciones, sino al derecho a la intimidad, por lo que pueden articularse como prueba aunque se hayan efectuado sin autorización judicial[409] .

[408] Conforme a la STC114/1984, de 29 de noviembre "*no hay secreto para aquél a quien la comunicación se dirige, no implica contravención de los dispuesto en el art.18.3 de la Constitución la retención, por cualquier medio, del contenido del mensaje, pues sobre los comunicantes no pesa el deber del secreto".*

[409] *Vid.* STC 56/2003, de 24 de marzo y SSTS 208/2006, de 20 de febrero; 1354/2005, de 16 de noviembre; 1564/1998, de 15 de diciembre.

La garantía del secreto de las comunicaciones sólo opera cuando la injerencia sea realizada por una persona ajena al proceso de comunicación. Como declara la STC 56/2003, de 24 de marzo "*la presencia de un elemento ajeno a aquéllos entre los que media el proceso de comunicación, es indispensable para configurar el ilícito constitucional aquí perfilado*".[410] Para esta resolución *"... no existe prohibición para conocer, por parte de uno de los interlocutores, el número de teléfono desde el que se establece comunicación con él; en otro caso todos los teléfonos que muestran el número desde el que están siendo llamados infringirían el secreto de las comunicaciones amparado por el art. 18.3 CE"*. Sólo podrá vulnerarse el derecho fundamental del art. 18.3 CE cuando se graba la conversación de otro, pero no cuando se graba una conversación con otro.

Esta doctrina jurisprudencial no se ve afectada por la circunstancia de que sea un tercero quien, con el consentimiento de uno de los interlocutores, grabe la conversación, como así señala la STS 298/2013, de 13 de marzo. El hecho de dicha Sentencia se refería no sólo al tercero en la grabación, sino también al engaño utilizado para llevarla a cabo, al hacerse pasar el tercero que grabó la comunicación por un abogado, cuando realmente era un investigador privado: "*la utilizabilidad de ese medio de prueba no queda supeditada a la conformidad en la grabación de todos los partícipes o contertulios; ni a la ausencia de toda connotación subrepticia o de engaño u ocultación por parte de quien dispone lo necesario para la fijación en un soporte de la conversación. Es suficiente que uno de los comunicantes o interlocutores preste su consentimiento para la intervención y grabación por un tercero para que resulte inoperante la cláusula de exclusión del art. 11 LOPJ. Es un elemento probatorio valorable. Sólo la escucha o grabación por un tercero sin autorización de ninguno de los comunicantes ni de la autoridad judicial convierte en inutilizable ese medio probatorio"*.

Como declara la STS 239/2010, de 24 de marzo, la grabación por uno de los interlocutores de la conversación telefónica "*no conculca secreto alguno impuesto por el art. 18.3 y tan sólo, acaso, podría concebirse como conducta preparatoria para la*

---

[410] Circular 1/2013 de la Fiscalía General del Estado en relación con la intervención de las comunicaciones.

ulterior difusión de lo grabado. Por lo que a esta última dimensión del comportamiento considerado se refiere, es también claro que la contravención constitucional sólo podría entenderse materializada por el hecho mismo de la difusión…Los resultados prácticos a que podría llevar tal imposición indiscriminada de una obligación de silencio al interlocutor son, como se comprende, del todo irrazonables y contradictorios, en definitiva, con la misma posibilidad de los procesos de libre comunicación humana".

A este respecto parece atinado el criterio[411] de que esta jurisprudencia pudiera ser desacertada al no haber establecido ningún requisito adicional para suspender la tranquilidad ciudadana y la intimidad de las personas de una forma tan agresiva. Y es que, a partir de la misma, podemos olvidarnos de tener ninguna conversación realmente privada, manteniéndola mejor a través de Telegram en modo de autodestrucción del mensaje. Sería bueno que se estableciera en qué situaciones se pueden grabar esas conversaciones por los propios interlocutores[412], o en su defecto, en qué casos se pueden hacer uso de las mismas.

4) Comunicante accidental.

El tercero o "comunicante accidental" se refiere a la persona que no es directamente investigada pero que entabla comunicación con el investigado. La propia naturaleza de la intervención determina que afecte no sólo al titular del terminal o del medio de comunicación, sino también a sus interlocutores[413].

[411] NIEVA FENOLL, J. La recuperación de la privacidad de las comunicaciones. http://noticias.juridicas.com/conocimiento/articulos-doctrinales/11095-la-recuperacion-de-la-privacidad-de-las-comunicaciones/ 25/05/2016 10:42:29.

[412] NIEVA FENOLL, J. La recuperación de la privacidad de las comunicaciones ob. cit. *La forma de deshacer ese evidente y rocambolesco absurdo consiste en determinar con precisión –y de forma simple– las situaciones en las que se pueden grabar esas conversaciones por los propios interlocutores. Esos casos debieran reducirse a un único supuesto: hechos delictivos que por su absoluta clandestinidad dejan en total indefensión y falta de pruebas a la víctima, y en los que solamente es la víctima quien puede obtener razonablemente las evidencias. El acoso sexual o la violencia sobre la mujer podrían ser buenos ejemplos."*

[413] SSTS 1001/2005, de 19 de julio y 1717/1999, de 3 de diciembre.

La intervención autorizada de las comunicaciones alcanza no solo a aquel cuya comunicación es observada, sino también al interlocutor que se relaciona con el primero, si la conversación se refiere a los hechos que conforman el delito investigado[414]. No puede considerarse constitucionalmente ilegítima la intervención de las conversaciones de las personas que comunican o con las que se comunican aquéllas sobre las que recaen inicialmente los indicios, en la medida en que tales conversaciones estén relacionadas con el delito investigado, correspondiendo al Juez, a través del control de la ejecución de la medida, la identificación de las conversaciones relevantes[415].

La STS 515/2006, de 4 de abril declara que en estos casos, la revelación del contenido de las conversaciones mantenidas con el inspeccionado no supone una vulneración del art. 18.3 CE, y así "…*por sus propias características toda comunicación telefónica precisa siempre de un mínimo de dos interlocutores, con independencia de quien sea el emisor o el receptor de la llamada, y la resolución judicial por la que se autoriza la escucha de las conversaciones recibidas o emitidas desde un terminal comprende necesariamente a ambos conversadores, en aras de alcanzar el objetivo de su adopción, esto es, averiguar si las fundadas sospechas se materializan en el descubrimiento del presunto ilícito investigado y de sus responsables".*

En conexión con este punto se plantea si es válido el material aportado cuando el usuario del teléfono intervenido cede el uso del mismo a un tercero[416], o cuando la intervención se realiza con base a la titularidad del terminal utilizado por un tercero. En

---

[414] Una intervención telefónica puede afectar los derechos de terceros ajenos a la investigación, sin que ello genere nulidades. La STS 433/2012, de 1 de junio puntualiza que la intervención afecta a las comunicaciones de las personas investigadas, pero puede suponer la inclusión como prueba de cargo las manifestaciones de los que se comuniquen con ellos, siempre que se refieran al hecho delictivo objeto de investigación.

[415] SSTS 712/2012, de 26 de septiembre; 751/2012, de 28 de septiembre; 493/2011, 26 de mayo; 309/2010, 31 de marzo.

[416] Para la STS 1362/2009, de 23 de diciembre, la autorización judicial para la intervención telefónica lo fue para las que se realizasen a través del teléfono indicado en la conversación inicial por los indicios de tráfico de drogas en la prisión a través del mismo. Si el teléfono es dejado a otra persona, relacionada y de acuerdo con el usuario habitual, para comunicarse sobre esa materia, esa comunicación está cubierta por las resoluciones judiciales de intervención de las comunicaciones a través de ese teléfono…la autorización judicial cubre las comunicaciones realizadas por el teléfono concernido, aunque lo utilicen otras personas no mencionadas en la resolución autorizante.

estos casos no hay lesión al derecho al secreto de las comunicaciones de ese tercero[417]. La utilización por varias personas de un terminal intervenido no exige una nueva autorización judicial. La STS 905/2003, de 18 de junio declara que "*lo relevante es que conste la identidad del titular del móvil para que la intervención sea correcta junto con los demás requisitos de uso constitucional, de suerte que la utilización esporádica de tal móvil por otra u otras personas del grupo implicado en la actividad delictiva no exige una nueva autorización de la intervención, en función de quien utilizase en cada momento el terminal".*

En relación con el tercero o comunicante accidental, el artículo 588 ter i LECrim apartado 3º, dispone que el juez de instrucción deberá notificar a las personas intervinientes en las comunicaciones interceptadas el hecho de la práctica de la injerencia, y se les informará de las concretas comunicaciones en las que haya participado que resulten afectadas, con tres excepciones: a) que sea imposible; b) que exija un esfuerzo desproporcionado o, c) puedan perjudicar futuras investigaciones..

Incluso, si la persona notificada lo solicita se le entregará copia de la grabación o transcripción de les comunicaciones, en la medida que esto no afecte al derecho a la intimidad de otras personas o resulte contrario a los fines del proceso en cuyo marco se hubiere adoptado la medida de injerencia (artículo 588 ter i LECrim, *in fine*).

[417] La STS 1319/2009, de 29 de diciembre considera que "*…la policía, salvo que hubiera realizado una escucha previa ilegal, no puede saber…cuál es el usuario habitual de un teléfono que ha contratado una persona perfectamente identificada. Es evidente que el derecho al secreto es personal y subjetivo. La petición judicial está cubierta por el dato evidente de la titularidad del teléfono".*

3.2.C) Procedimiento para intervenir las comunicaciones.

El procedimiento para la interceptación de comunicaciones telefónicas y telemáticas desde la solicitud y las actuaciones posteriores relativas a la medida solicitada, se sustanciarán en una pieza separada y secreta, sin necesidad de que se acuerde expresamente el secreto de la causa, de conformidad con el artículo 588 bis d de la LECrim, común al resto de medidas de investigación tecnológica[418].

Para que la diligencia de intervención de las comunicaciones sea eficaz ha de estar acompañada necesariamente del secreto de las actuaciones, como único medio de soslayar el derecho de todo investigado desde el principio, a intervenir y a ejercer el derecho de defensa como concede el art. 118 LECrim (STS 182/2004, de 23 de abril)[419]. En esta misma línea, la STS 704/2009, de 29 de junio declara que como elemento esencial implícito a la misma y presupuesto de su efectividad y utilidad, debe entenderse comprendido el secreto de la diligencia de intervención telefónica, no sólo por la necesidad inmanente de la propia diligencia, sino porque su notificación le privaría de practicidad a la misma y uno de los condicionamientos de la medida injerencial es su utilidad, y el juez no puede contradecirse dictando una medida inútil, que por tal razón sería improcedente e inadecuada[420].

[418] Desde hace unos años, la intervención de las comunicaciones telefónicas en España se lleva a cabo por medio de SITEL (Sistema de Interceptación de Telecomunicaciones), configurado con un sistema de enlaces punto a punto con las operadoras de telefonía, que transmiten directamente las intervenciones autorizadas, las cuales son almacenadas de manera automática, íntegramente y bajo firma digital, en el mismo formato remitido, esto es, sin intervención alguna de los agentes facultados. El proceso culmina con el volcado de estos archivos en un soporte físico (DVD o CD), para su entrega al órgano jurisdiccional. Sin embargo, determinados servicios de comunicación (WhatsApp, Gmail, etc.) gestionados por entidades domiciliadas fuera de España no podrán ser intervenidos por esta vía, debiendo acudirse a los mecanismos de cooperación internacional cuya lentitud restará eficacia a la diligencia. Ello podrá abrir camino a otros recursos más ágiles y provechosos como el acceso remoto a dispositivos, que será analizado más adelante.

[419] Informe del Consejo Fiscal sobre el anteproyecto de reforma de la LECrim. Debe recordarse que existe una línea jurisprudencial que defiende que la decisión de proceder a unas intervenciones telefónicas lleva implícita la declaración de secreto de las actuaciones por definición y por elementales exigencias de la lógica (SSTS 940/2008, de 18 de diciembre;1090/2005, de 15 de septiembre) pues "*sería absurdo avisar a alguien de que se le va a intervenir su teléfono"* (STS 738/1996, de 11 de octubre).

[420] En el mismo sentido se pronuncia la STS 1044/2011, de 11 de octubre.

1) Resolución Judicial.

Para adoptar esta medida de investigación tecnológica será preceptiva la autorización judicial en forma de auto motivado. Con la excepcional salvedad, de que en caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas y existan razones fundadas que hagan imprescindible esta medida, podrá ordenarla el Ministro del Interior o, en su defecto, el Secretario de Estado de Seguridad. En este caso, se comunicará inmediatamente al juez competente, dentro del plazo máximo de veinticuatro horas, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado, para que revoque o confirme tal actuación en un plazo máximo de setenta y dos horas desde que fue ordenada la medida[421].

Salvo esta excepción, la regla general es que esta medida de investigación tecnológica sea adoptada mediante auto motivado, de oficio o a instancia de la policía o del Ministerio Fiscal, cuya solicitud deberá contener según el articulo 588 ter d:

a) la identificación del número de abonado, del terminal o de la etiqueta técnica,

b) la identificación de la conexión objeto de la intervención o

c) los datos necesarios para identificar el medio de telecomunicación de que se trate.

También podrá tener por objeto dicha solicitud alguno de los siguientes extremos, para determinar la extensión de la medida:

a) El registro y la grabación del contenido de la comunicación, con indicación de la forma o tipo de comunicaciones a las que afecta.

b) El conocimiento de su origen o destino, en el momento en el que la comunicación se realiza.

[421] Artículo 588 ter d. Párrafo Tercero.

c) La localización geográfica del origen o destino de la comunicación.

d) El conocimiento de otros datos de tráfico asociados o no asociados pero de valor añadido a la comunicación. En este caso, la solicitud especificará los datos concretos que hayan de ser obtenidos.

El juez de instrucción autorizará o denegará la medida solicitada mediante auto motivado[422], oído el Ministerio Fiscal, que dictará en el plazo máximo de veinticuatro horas desde que se presente la solicitud, con el contenido ya indicado en el artículo 588 bis c de la LECrim.

Con esta regulación tan precisa que contiene la LECrim acerca del contenido del auto y su motivación no tendría cabida la llamada motivación por remisión, que aunque no sin críticas, la jurisprudencia, había venido admitiendo, dando validez a las resoluciones judiciales que autorizaban la intervención de las comunicaciones limitándose en su motivación a realizar una remisión a los hechos e indicios recogidos

[422] Respecto a los posibles errores por parte del auto autorizante, si bien es cierto que la LECrim, tras la reforma operada por LO 13/2015, exige que la autorización judicial determine y delimite el alcance de la medida, una mención oscura o errónea en el auto de intervención de comunicaciones puede ser interpretada de manera racional, de modo tal que debamos entender que una limitación de las comunicaciones a intervenir en una línea, exige una motivación o fundamento que lo justifique. Esto es lo que viene a señalar la STS 90/2010, de 5 de febrero, en relación con la limitación de las llamadas entrantes de un teléfono: "se declaró por la Audiencia, así mismo, la nulidad de los resultados obtenidos con las intervenciones por el hecho de que se hubiera excedido por los funcionarios encargados de la práctica de la diligencia el ámbito de la autorización judicial, al interceptar todas las conversaciones realizadas a través de las líneas intervenidas cuando lo cierto es que las prórrogas tan sólo se refieren a las llamadas "efectuadas por el usuario", lo que se interpreta como un permiso limitado, tan sólo, a las llamadas "salientes" del terminal mencionado, pero no a las "entrantes". El absurdo de una tal interpretación, respecto de una expresión realmente insólita en esta materia, máxime cuando los Autos iniciales no contenían tal frase, obliga a que, en servicio de la más estricta racionalidad, se entienda que la verdadera voluntad del Instructor, aunque defectuosamente expresada, aludía en realidad a la interceptación de aquellas conversaciones que se realizasen mediante la línea telefónica objeto de la diligencia. En efecto, no tendría sentido alguno, ni fundamento práctico ni jurídico, el que sólo se pudiera tomar conocimiento de lo conversado por el usuario del terminal telefónico cuando él daba inicio a la llamada, cualquiera que fuere su interlocutor, y a la vez no estuviera autorizado tener constancia, en el transcurso de una investigación criminal de estas características, del contenido de las conversaciones mantenidas por este mismo investigado cuando fuera él el destinatario de la llamada, al no existir además razonamiento alguno en la Resolución autorizante explicativo de tan peculiar ámbito de la diligencia. Por ello ha de considerarse plenamente razonable la interpretación realizada por los funcionarios autorizados que, por otra parte, no fue en ningún momento corregida con posterioridad por el propio Instructor autor de semejante autorización".

en el oficio policial que había sido presentado en el Juzgado, sin recoger expresamente el auto tales hechos e indicios[423].

De otra parte, la adopción de este tipo de medida requiere que se haya oído con carácter previo al Ministerio Fiscal. No basta con la posterior notificación del auto que acuerde la medida, sino que se precisa que se dé audiencia al fiscal antes de su adopción, planteándose serias dudas al respecto sobre si esta falta de audiencia podría suponer un vicio procesal de dimensión constitucional que invalidara los resultados obtenidos mediante éstas y las consecuencias probatorias derivadas, directa e indirectamente, de las mismas, por aplicación del artículo 11.1 de la Ley Orgánica del Poder Judicial[424].

Por otra parte, la LECrim establece un deber de colaboración y de guardar secreto por parte de los operadores cuyo incumplimiento será constitutivo de un delito

[423] Claro exponente de esta doctrina jurisprudencial, es la STS 745/2015, de 23 de noviembre cuando señala que "tanto el Tribunal Constitucional como esta misma Sala (SSTC 123/1997, de 1 de julio, 165/2005, de 20 de junio, 261/2005, de 24 de octubre, 26/2006, de 30 de enero, 146/2006, de 8 de mayo y 72/2010, de 18 de octubre, entre otras, y SSTS de 6 de mayo de 1997, 14 de abril y 27 de noviembre de 1998, 19 de mayo del 2000, 11 de mayo de 2001, 3 de febrero y 16 de diciembre de 2004, 13 y 20 de junio de 2006, 9 de abril de 2007, 248/2012, de 12 de abril y 492/2012, de 14 de junio, entre otras), han estimado suficiente que la motivación fáctica de este tipo de resoluciones se fundamente en la remisión a los correspondientes antecedentes obrantes en las actuaciones y concretamente a los elementos fácticos que consten en la correspondiente solicitud policial, o en el informe o dictamen del Ministerio Fiscal, cuando se ha solicitado y emitido (STS 248/2012, de 12 de abril). La motivación por remisión no es una técnica jurisdiccional modélica, pues la autorización judicial debería ser autosuficiente (STS núm. 636/2012, de 13 de julio y STS 301/2013, de 18 de abril). Pero la doctrina constitucional admite que la resolución judicial pueda considerarse suficientemente motivada sí, integrada con la solicitud policial, a la que se remite, o con el informe o dictamen del Ministerio Fiscal en el que solicita la intervención (STS núm. 248/2012, de 12 de abril), contiene todos los elementos necesarios para llevar a cabo el juicio de proporcionalidad (doctrina jurisprudencial ya citada, por todas STC 72/2010, de 18 de octubre)".

[424] En este sentido pudiera ser de aplicación la jurisprudencia sobre la falta de notificación del auto de intervención telefónica al Ministerio Fiscal. En un primer momento existió una línea jurisprudencial seguida por el Tribunal Constitucional que consideraba nula una intervención telefónica por falta de notificación del auto habilitante al Ministerio Fiscal. Posteriormente fue superada por la jurisprudencia posterior, de la que es claro exponente la STS 90/2010, de 5 de febrero, cuando establece que "en primer lugar, se nos dice que la ausencia de notificación formal al Fiscal de la autorización de tales diligencias supone un vicio procesal de dimensión constitucional que invalida los resultados obtenidos mediante éstas y las consecuencias probatorias derivadas, directa e indirectamente, de las mismas, por aplicación del artículo 11.1 de la Ley Orgánica del Poder Judicial. Pero, frente a ello, la doctrina pacífica de esta Sala, de la que puede servir de ejemplo la STS 203/2007 de 13 de marzo, viene insistiendo en lo siguiente: *"...hemos de recordar que cualquier deficiencia formal en el proceso para que posea capacidad invalidante ha de provocar una material indefensión a alguna de las partes, cosa que en este caso no ocurre. El Fiscal es inspector de cualquier causa penal incoada o en tramitación conforme al art. 306 LECrim y ha tenido oportunidad de intervenir en todo momento. Pero además, aunque en el instante de dictarse no se haya notificado alguna diligencia, no le priva del derecho a recurrirla en cualquier momento una vez hecha la notificación. En cualquier caso, la garantía de las decisiones injerenciales reside en el juez que las dicta y no en la notificación al Fiscal".*

de desobediencia, por lo que el auto que apruebe la intervención de las comunicaciones deber hacer mención a estos deberes con el apercibimiento de desobediencia (art. 588 ter e LECrim).

2) Duración y prórroga.

Se establece un plazo de tres meses como duración máxima inicial de la intervención, plazo que es susceptible de ampliación y prórroga, previa petición razonada por períodos sucesivos de igual duración, hasta un máximo temporal de dieciocho meses, siempre que subsistan las causas que motivaron aquella (artículo 588 ter g LECrim).

En lo referente a la duración, no es aventurado afirmar que, si bien el 588 bis e LECrim la hace depender del carácter de cada medida, el límite máximo de dieciocho meses establecido en las telecomunicaciones actuará de tope también en las otras.

Como acertadamente apunta algún autor[425], resulta difícil conciliar el secreto de las actuaciones y el plazo de intervención. Para la fundamentación de la solicitud de la prórroga, la Policía Judicial aportará, un informe detallado del resultado de la medida, las razones que justifiquen la continuación de la misma en su caso, con la transcripción de aquellos pasajes de las conversaciones de las que se deduzcan informaciones relevantes para decidir sobre el mantenimiento de la medida (artículo 588 ter h LECrim). De esta forma se busca un equilibrio entre la necesidad de valerse de estas diligencias para la investigación de los delitos más graves para la sociedad y la importancia de definir unos límites cronológicos que no prolonguen de forma innecesaria la interferencia de los poderes públicos en la privacidad de los ciudadanos afectados por la medida. En el plazo de los dos días siguientes a la presentación de la solicitud, el juez resolverá sobre el fin de la medida o su prórroga mediante auto

[425] GONZÁLEZ-MONTES SÁNCHEZ J.L. "Reflexiones sobre el Proyecto de Ley Orgánica de modificación de la LECrim para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas". Revista electrónica de ciencia penal y criminología nº 17-06, junio 2015.

motivado. Antes de dictar la resolución podrá solicitar aclaraciones o mayor información. Concedida la prórroga, su cómputo se iniciará desde la fecha de expiración del plazo de la medida acordada de conformidad con el artículo 588 bis f.

3) Control y cese de la medida.

Con el fin de asegurar la autenticidad e integridad de los soportes puestos a disposición del juez, se impone la utilización de un sistema de sellado o firma electrónica que garantice la información volcada desde el sistema central. Esta medida es paralela a la exigida en otros órdenes jurisdiccionales para la plena validez de los documentos aportados al proceso en formato electrónico y acoge una línea jurisprudencial de la Sala Segunda del Tribunal Supremo (art. 588 ter f LECrim).

Dada la gravedad de la injerencia en la intimidad del sujeto pasivo de la medida, el juez deberá estar en contacto con la policía judicial para controlar su desarrollo y resultados, cesándola cuando desaparezcan las causas que motivaron su adopción, devenga ineficaz o haya transcurrido el plazo[426].

Tras cesar la media se entregará a las partes el material interceptado, mediante copia íntegra de la grabación y transcripción de los pasajes que considere de interés (artículo 588 ter i LECrim). Respecto a la transcripción de la grabación la STS 40/2009, de 28 de enero, compendia la doctrina jurisprudencial, al señalar " *esta Sala ha dicho también (Cfr. STS 353/2007, de 7 de mayo), que la transcripción no es un requisito impuesto por la ley, y que en lo referente a las transcripciones de las cintas, estas solo constituyen un medio contingente -y por tanto prescindible- que facilita la consulta y constatación de las cintas, por lo que sólo éstas son las imprescindibles. No existe ningún precepto que exija la transcripción ni completa ni parcial de los pasajes más relevantes, ahora bien, si se utilizan las transcripciones, su autenticidad, solo vendrá acreditada si están debidamente cotejadas bajo la fe del Secretario Judicial (Cfr. STS*

[426] GIMENO BEVIÁ, J. "Análisis crítico de la reforma de la LECrim 2015 (…)" ob. cit. pág. 9.

538/2001, de 21 de marzo; STS 650/2000, de 14 de septiembre; STS 209/2007, de 9 de marzo)[427].

Si bien es cierto que el ejercicio del derecho de defensa de las partes comprende la necesidad de que con anterioridad a la celebración del juicio oral le sean entregadas copias de las grabaciones de las comunicaciones telefónicas obrantes en las actuaciones, no se trata de un derecho absoluto, habiendo sido matizado por nuestra jurisprudencia en diversas ocasiones cuando no se produce quiebra del derecho a la tutela judicial efectiva y siempre que se garantice debidamente el derecho de las partes a tener acceso a dichos documentos[428].

La LECrim tras la reforma del 2015 solo exige que en caso que no se incluya la totalidad de la grabación en la transcripción entregada se haga constar de modo expreso. Cuando sean examinadas las grabaciones y en el plazo fijado por el juez, en atención al volumen de la información contenida en los soportes, cualquiera de las partes podrá solicitar la inclusión en las copias de aquellas comunicaciones que entienda relevantes y hayan sido excluidas. El juez de instrucción, oídas o examinadas por sí esas comunicaciones, decidirá sobre su exclusión o incorporación a la causa (art. 588 ter i 2 LECrim).

[427] La STS 833/2001 de 14 de mayo, señala que "*no es correcto identificar el control judicial con dicha transcripción, tal identificación no tiene en cuenta que el material probatorio son las cintas grabadas, no su transcripción. En todo caso, la transcripción tiene la misión de permitir el acceso al contenido de las cintas mediante la lectura, pero no es un elemento que integre la diligencia con carácter necesario y legítimamente. La Ley procesal no exige esta transcripción en el art. 579 LECrim y su realización obedece más a la costumbre que a las necesidades de control judicial. Esto por otra parte, se satisface en primer lugar mediante las autorizaciones motivadas que requiere la disposición antes ya citada y por la comprobación del carácter integro de las grabaciones. Es claro que la transcripción no sustituye la audición de las cintas en el juicio oral caso de que las partes lo soliciten para comprobar si las transcripciones que obran en las actas de instrucción son o no completas para valerse de ellas su defensa. En todo caso, a diferencia de las exigencias de resolución motivada, proporcionalidad de la medida y previa existencia de indicios que condicionan la legitimidad constitucional, la cuestión del control judicial de la intervención pertenece al ámbito de la legislación ordinaria por lo que su hipotética infracción no origina vulneración de derechos constitucionales ni afectación de otros elementos de prueba derivados de ella, y la audición integra de las cintas en el plenario constituye la practica contradictoria de la prueba, que subsana aquellas".*

[428] La STS 165/2013, de 26 de marzo, desestima un recurso de casación interpuesto por no haber sido entregadas tales copias estableciendo que "*debe señalarse que han estado (las cintas) a lo largo de esta fase del procedimiento a su disposición, y que resulta desproporcionada su pretensión de que se le facilite la copia íntegra de todas las grabaciones. En definitiva, ninguna quiebra al derecho a la obtención de la tutela judicial efectiva y del derecho de defensa puede anudarse al hecho de que no se facilitasen gratis - pues eso es lo que se solicita- las copias de las cintas. La respuesta del Juzgado de carecer de medios es sensata y razonable. Procede la desestimación de ambos motivos".*

Esta posibilidad de las partes de verificar la falta de relevancia de las comunicaciones no incluidas mediante el examen de la grabación es absolutamente esencial para garantizar el derecho de defensa, evitar desconfianzas y recelos y, en definitiva, reducir la litigiosidad[429].

Por último, especial mención merece en esta diligencia de investigación la destrucción de archivos (art. 588 bis k). Se pretende con ello evitar toda difusión de un material que, por su propio contenido, podría dañar de forma irreparable la intimidad del afectado. Conviene poner de relieve que la custodia no es competencia judicial sino de los Letrados al servicio de la Administración de Justicia, quienes conservarán una copia que deberá ser destruida a los cinco años salvo que fuera precisa su conservación[430]. Se trata, por tanto, de una medida necesaria y útil para evitar posibles filtraciones, pues no es de recibo que las comunicaciones privadas permanezcan *per secula seculorum* al alcance de los miembros de la oficina judicial[431].

La previsión es acorde con la jurisprudencia del TS: "*los Tribunales en las causas en las que se haya procedido a la realización de intervenciones telefónicas, deberán acordar de oficio en sus sentencias la destrucción de las grabaciones originales que existan en la unidad central del sistema SITEL y de todas las copias, conservando solamente de forma segura las entregadas a la autoridad judicial, y verificando en ejecución de sentencia, una vez firme, que tal destrucción se ha producido*"(STS 565/2011, de 6 de junio)[432].

[429] Informe del Consejo Fiscal sobre el anteproyecto de reforma de la LECrim.

[430] RODRÍGUEZ LAÍNZ, J L. "Análisis del espectro electromagnético de señales inalámbricas: rastreo de dispositivos Wi-Fi". Diario La Ley nº 8588, Sección doctrina, 2015. pág. 26

[431] GIMENO BEVIÁ, J. "Análisis crítico de la reforma de la LECrim 2015 (…)". ob. cit. pág. 9.

[432] SSTS 293/2011, de 14 de abril; 380/2012, de 16 de mayo; 410/2012, de 17 de mayo; 794/2012, de 11 de octubre y 143/2013, de 28 de febrero, han establecido categóricamente que: "*Los tribunales deberán de oficio acordar en sus sentencias la destrucción de las grabaciones originales que existían en el centro de recepción y de todas las copias, conservando solamente de forma segura las copias entregadas a la autoridad judicial; y verificando en ejecución de la sentencia, una vez firme, que la destrucción se ha producido".*

3.3. El registro de dispositivos de almacenamiento masivo de la información.

3.3.A) Naturaleza jurídica de los dispositivos informáticos.

Esta diligencia permite el acceso a la información contenida en ordenadores, discos duros, USB, teléfonos móviles y demás dispositivos de almacenamiento masivo.

Al hablar de dispositivos de almacenamiento masivo de la información se hace referencia tanto a ordenadores o instrumentos de comunicación telefónica o telemática, como a dispositivos de almacenamiento masivo de información digital como discos duros, USB, CD, DVD, etc.. o el acceso a repositorios telemáticos de datos.

Una primera cuestión que conviene determinar es la naturaleza jurídica de estos dispositivos. Pueden considerarse desde meros equipos técnicos de trabajo y almacenamiento de los datos informáticos, o bien, como un "domicilio informático" independiente del lugar donde se ubique físicamente, susceptible de integrar parte esencial del ámbito de la privacidad personal, y por tanto afecto a los principios de protección y salvaguarda de la intimidad constitucionalmente amparables[433].

El Tribunal Constitucional[434] considera el ordenador personal como un "medio idóneo" para albergar contenidos relativos a nuestra intimidad[435], lo que le lleva a

[433] AGUSTINA SANLLEHÍ, J R. "Interrogantes en torno a las diligencias preliminares ante la ciberdelincuencia. Sobre la garantía del derecho a la intimidad en el registro del ordenador (a propósito de la STC 173/2011)". La ley penal jurisprudencia nº 98-99, noviembre-diciembre 2012, pág. 91.

[434] El Tribunal Constitucional parte de la premisa de que "*un ordenador personal puede ser un medio idóneo para el ejercicio de la intimidad personal, resultando entonces necesario para acceder a su contenido el consentimiento de su titular o que se den los presupuestos que legalmente habilitan la intromisión, de acuerdo con los parámetros constitucionales antes desarrollados"* (STC 173/2011, de 7 de noviembre [FJ 3º].

[435] La STC 173/2011, de 7 de noviembre establece que "*el cúmulo de la información que se almacena por su titular en un ordenador personal, entre otros datos sobre su vida privada y profesional (en forma de documentos, carpetas, fotografías, vídeos, etc.) por lo que sus funciones podrían equipararse a los de una agenda electrónica, no sólo forma parte de este mismo ámbito, sino que además a través de su observación por los demás pueden descubrirse aspectos de la esfera más íntima del ser humano. Es evidente que cuando su titular navega por Internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico, forma parte de grupos de noticias, entre otras posibilidades, está revelando datos acerca de su personalidad, que pueden afectar al*

afirmar como regla general que cualquier registro del mismo debe contar con autorización del titular (aun tácita, derivada de actos concluyentes), o bien con autorización judicial. Dicha regla, no obstante, pudiera ser excepcionada cuando, previa habilitación legal, la intromisión resulte urgente necesaria, adecuada y proporcionada para salvaguardar otros bienes constitucionalmente valiosos[436].

La STEDH de 3 de abril de 2007 caso *Copland c.* Reino Unido señaló que debían incluirse en la protección del artículo 8 del Convenio Europeo de Derechos Humanos "*la información derivada del seguimiento del uso personal de internet"*. Según el Tribunal Supremo, "esos archivos pueden contener datos sensibles en orden a la intimidad, en la medida que pueden incorporar informaciones reveladores sobre determinados aspectos de la vida privada (ideología, orientación sexual, aficiones personales, etc.)" (STS, sala de lo social, de 26 de septiembre de 2007, rec. 966/2006 [FJ 4º].

En este sentido se pronunció la Circular de la Fiscalía General del Estado 1/2013 sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas: "*se ha puesto de manifiesto que, a pesar de las múltiples funciones tanto de recopilación y almacenamiento de datos como de comunicación con terceros a través de internet que posee un ordenador personal, el acceso a su contenido podrá afectar bien al derecho a la intimidad personal (art. 18.1 CE), bien al derecho al secreto de las comunicaciones (art. 18.3 CE) en función de si lo que resulta desvelado a terceros son, respectivamente, datos personales o datos relativos a la comunicación... Lo determinante para la delimitación del contenido de los derechos fundamentales recogidos en los arts. 18.1 y 18.3 CE no es el tipo de soporte, físico o electrónico, en el que la agenda de contactos esté alojada ni el hecho, de que la agenda sea una aplicación de un terminal telefónico móvil, que es un instrumento de y para la comunicación, sino el carácter de la información a la que se accede"*.

---

núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc. Quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona" [FJ 3º, *in fine*].

[436] *Artículo 588 sexies c apartados 3º y 4º.*

La normativa que regía la ejecución de la injerencia sobre los archivos (no comunicaciones) encontrados en los dispositivos almacenadores de memoria en las nuevas tecnologías, incluidos los discos duros, era la propia del derecho a la intimidad (art. 18.1 CE)[437] y por ello su desarrollo se resumía en la posibilidad de su ocupación, siempre que hubiera sido prevista y autorizada en el correspondiente auto de entrada y registro[438].

Por lo que respecta a la correspondencia ya abierta y conocida por parte del investigado, dejaba de serlo a los efectos del título VIII del libro II de la LECrim[439], y se transforma en fuente de prueba documental -contenga o no información íntima- que puede perfectamente aprehenderse tras su visionado en el lugar del registro (pues es en el auto que lo autoriza donde se ha ponderado y admitido su injerencia, exteriorizando la necesidad de su ocupación) o posterior estudio en dependencias policiales por los comisionados del juez ordenante del registro. En caso de que fuera correo no leído por el receptor requiere entonces autorización judicial al afectar al derecho del artículo 18.3 de la CE.

Es necesario tener en cuenta que el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado, no sólo el derecho al secreto de las comunicaciones del art. 18.3 CE (por cuanto es indudable que la utilización de este procedimiento supone un acto de comunicación), sino también el derecho a la intimidad personal (art. 18.1 CE), en la medida en que estos correos o e-mail, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado (STC 173/2011, de 7 de noviembre). Por ello, el TC entiende que afectará al secreto de las comunicaciones el acceso a cualquier función del teléfono móvil que pudiera desvelar procesos comunicativos (STC 115/2013, [FJ 4º], lo que puede extenderse a cualquier dispositivo electrónico.

---

[437] AGUSTINA SANLLEHÍ, JR. "Interrogantes en torno a las diligencias preliminares ante la ciberdelincuencia (…)". ob. cit. pág. 91.

[438] STS 1094/2010 de 10 de diciembrebre, STS 1934/2000 de 12 de diciembre.

[439] La STS 1235/2002 de 27 de junio, permite la lectura de un mensaje grabado en un móvil porque se encuentra bajo la cobertura de la autorización judicial como si de otro papel o documento se tratara, pues se hace en el curso de su incautación en la entrada y registro. En el mismo sentido, la SAP Cáceres sección 2º, 84/2004 de 17 de junio "*el auto posibilita por el contenido del mismo, el comiso del ordenador o de los contenidos del mismo, y por lo tanto no podemos entender que se ha vulnerado el derecho al secreto de las comunicaciones con la actividad realizada".*

En definitiva, el acceso al contenido de los dispositivos electrónicos puede afectar al secreto de las comunicaciones en aquellos supuestos en los mismos sean utilizados para el proceso de transmisión de información entre un transmisor y un receptor a través de redes de comunicación abiertas o restringidas como internet, telefonía fija, móvil u otras[440]. Así ocurre con el correo electrónico, la mensajería instantánea o similar (conversaciones de chat, mensajes cortos y otros supuestos de análoga naturaleza), tanto desde la perspectiva de la existencia de norma legal habilitante, como desde la perspectiva de si la concreta actuación desarrollada se ha ejecutado respetando escrupulosamente el principio de proporcionalidad (STC 142/2012, de 7 de julio).

Frente a los esfuerzos por diferenciar los derechos fundamentales afectados en función de la naturaleza de cada uno de los contenidos albergados en un ordenador, la STS 342/2013, de 17 de abril, se decanta por una tesis unitaria del reconocimiento del derecho a la identidad virtual: "*la ponderación judicial de las razones que justifican, en el marco de una investigación penal, el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de vista la multifuncionalidad de los datos que se almacenan en aquel dispositivo. Incluso su tratamiento jurídico puede llegar a ser más adecuado si los mensajes, las imágenes, los documentos y, en general, todos los datos reveladores del perfil personal, reservado o íntimo de cualquier encausado, se contemplan de forma unitaria. Y es que, más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual"*[441].

Llama poderosamente la atención que con anterioridad a 2015, el registro e incautación de sistemas informáticos o datos informáticos no estaba previsto de forma expresa en la LECrim. Se aplicaban las normas generales relativas al registro domiciliario (arts. 567 y ss) y en particular los relativos al registro e intervención de libros, papeles y efectos del delito (arts. 573 a 578). Era el equivalente digital de la tradicional entrada y registro de domicilio con recogida de los instrumentos y efectos del delito y en consecuencia la única garantía judicial necesaria para llegar al contenido

[440] DELGADO MARTIN, J, "Derechos fundamentales afectados en el acceso al (…) ob. cit. pág. 1-20.

[441] En el mismo sentido la STS 204/2016, de 10 de marzo, que consagra el derecho constitucional de nueva generación constitutivo de una protección del propio entorno virtual.

de un ordenador ubicado en un domicilio privado era exclusivamente el auto de autorización de entrada y registro, pues con él se permitía lícitamente:

- la entrada en un lugar cerrado en que se desarrolla vida privada, aun contra la voluntad de su ocupante.
- El registro de todas sus dependencias y pertenencias,
- la ocupación de lo necesario y conducente a la investigación autorizada por el juez, y entre las que se hallan las comunicaciones pasadas y los documentos escritos, gráficos o audiovisuales necesarios, en cualquier tipo de soporte que se encuentren.

La vigente regulación de la LECrim (arts. 588 sexies a, b y c) descarta cualquier duda acerca de que esos instrumentos de comunicación y, en su caso, almacenamiento de información son algo más que simples piezas de convicción, de ahí la exigente regulación respecto del acceso a su contenido, en la que no basta con el simple auto de entrada y registro para acceder al contenido de estos dispositivos, sino que precisa que se detalle en dicho auto, caso de estar en domicilio, las razones que justifican el acceso al contenido de lo incautado. En definitiva, la policía podrá incautar los dispositivos, pero para el caso de acceder al contenido de ellos precisa autorización judicial propia y específica. Es decir, se precisará una segunda autorización.

3.3.B) Autorización requerida en función de su ubicación.

El registro de dispositivos de almacenamiento masivo de información tiene una regulación independiente en función de que el dispositivo se encuentre en un domicilio o fuera de él:

- Dentro un registro domiciliario: cuando con ocasión de la práctica de un registro domiciliario sea previsible la aprehensión de ordenadores, instrumentos de comunicación telefónica o telemática o dispositivos de almacenamiento masivo de información digital o el acceso a repositorios telemáticos de datos, la resolución del juez de instrucción habrá de extender su razonamiento a la justificación, en su caso, de las

razones que legitiman el acceso de los agentes facultados a la información contenida en tales dispositivos (art. 588 sexies a LECrim).

Se hace necesario acordar en el mismo auto de entrada y registro, razonándolo *ad casum,* la intervención de las comunicaciones privadas que se encuentren entre lo aprehendido y la concreción de la pericia, para el caso de incautarse dispositivos almacenadores de memoria (CD, DVD, discos duros, USB, etc.). La autorización judicial para efectuar el registro de un domicilio no supone *per se* el acceso a todo lo que se encuentre dentro del mismo[442]. Por consiguiente, para el acceso a dichos dispositivos, repositorios telemáticos de datos, ordenadores, teléfonos, etc, el art. 588 sexies a requiere que el juez motive, de forma individualizada el referido acceso, pues la mera incautación no otorga, legitima el acceso a su contenido, sin perjuicio de que posteriormente el juez pueda autorizar a dicho acceso.

- Fuera de un registro domiciliario: será necesario contar con autorización judicial motivada en aquellos supuestos en los que los ordenadores, instrumentos de comunicación o dispositivos de almacenamiento masivo de datos, o el acceso a repositorios telemáticos de datos, sean aprehendidos con independencia de un registro domiciliario. En tales casos, los agentes pondrán en conocimiento del juez la incautación de tales efectos. Si éste considera indispensable el acceso a la información albergada en su contenido, otorgará la correspondiente autorización (art. 588 sexies b LECrim).

Cuando la aprehensión del dispositivo se produzca fuera de lugares considerados "domicilio", también se deberán respetar las mismas garantías que el anterior por lo que, el tratamiento individualizado con respecto al primer supuesto no tiene demasiado sentido, y el legislador quizá hubiera podido realizarlo conjuntamente[443].

- Excepción en los casos de urgencia en que se aprecie un interés constitucional legítimo que haga imprescindible el acceso al contenido de los dispositivos (art. 588

[442] GIMENO BEVIÁ, J. "Análisis crítico de la reforma de la LECrim 2015 (…)". ob. cit. pág. 11.
"*En materia de derechos fundamentales no cabe la máxima de "quien puede lo más, puede lo menos porque, en la actualidad, puede afectarse más a la intimidad en el examen de un dispositivo de almacenamiento o "Pen drive" que en el registro de un domicilio".*

[443] GIMENO BEVIÁ, J. "Análisis crítico de la reforma de la LECrim 2015 (…)". ob. cit. pág. 11.

sexies c apartado 4º). La Policía Judicial podrá llevar a cabo el examen directo de los datos contenidos en el dispositivo incautado, comunicándolo inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, por escrito motivado al juez competente, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado[444]. El juez

[444] *Vid*. DELGADO MARTIN, J, "Derechos fundamentales afectados en el acceso al (…)". ob. cit. pág. 8 análisis de la Sentencia del Tribunal Constitucional 173/2011, de 7 de noviembre, se deniega al recurrente, condenado por un delito de distribución de pornografía infantil en internet, su petición de considerar que la Policía vulneró su derecho a la intimidad al registrar sin autorización judicial su ordenador portátil. "*Podría decirse que nos hallamos ante una colisión de derechos fundamentales y otros intereses constitucionalmente protegidos (intimidad versus intereses en la investigación criminal), en los que sería aplicable la doctrina general de la proporcionalidad (vid., entre otras, STC n 70/2002, de 3 de abril, FJ 10; STC 207/1996, de 16 de diciembre, FJ 4; STC 89/2006, de 27 de marzo, FJ 3)*. El Tribunal Constitucional (*vid.* [FJ 7] STC 173/2011) entiende que la actuación de la Policía fue necesaria y proporcional. Se debería haber legitimado la actuación policial en el contexto de lo que podría denominarse un procedimiento rutinario de verificación y aseguramiento del cuerpo del delito y no en el carácter de urgencia. No estaríamos, de este modo, ante una invasión intrusiva ilegítima, sino ante un proceder ordinario que es consecuencia de la evidencia de un hecho delictivo flagrante. Y ello sin perjuicio de que el usuario del ordenador fuera o no responsable criminalmente del almacenamiento de dichas imágenes en su ordenador. Es decir, la secuencia lógica y razonable de los hechos lleva a considerar que el precedente hallazgo casual justificaba y daba plena cobertura jurídica al posterior registro del ordenador, a pesar de que ello pudiera afectar, lógicamente, la intimidad del recurrente.
Otra teoría aun rechazando la tesis sostenida anteriormente sobre el carácter rutinario del registro policial en caso de delito flagrante, se podría haber argumentado la no exclusión de la prueba del proceso, a pesar de considerar que sí hubo violación de la intimidad, con base en algunas excepciones a la regla general de la inadmisibilidad de las pruebas ilícitas. De este modo, en el caso analizado en la STC 173/2011 sí se puede afirmar, fuera de toda duda, que el resultado probatorio hubiera sido el mismo, con o sin autorización judicial.
Se analiza la línea de argumentación sostenida en la STC 173/2011, y se se sugiere un reenfoque de la materia a partir de las facultades de la policía para aprehender los objetos del delito. Se abordan, en realidad, dos problemas claramente diferenciados. En cuanto al primero, se trata de profundizar en los argumentos para sostener que la intimidad no estaba comprometida y que, si lo estaba, concurrían razones que justificaban la intervención policial. En cuanto al segundo, de forma subsidiaria se ha sostenido que, aun en el caso de se llegara a considerar que sí hubo prueba ilícita, concurrían también razones para excepcionar el principio de inadmisibilidad consagrado en el art. 11 LOPJ.
Ambas líneas argumentativas son plausibles, bien para, en primer lugar, justificar la actuación policial, o, en su defecto, para excepcionar la expulsión del proceso de las pruebas obtenidas de conformidad con los principios de buena fe e inevitabilidad del descubrimiento.
En definitiva, dicha injerencia estuvo justificada, dependerá de si existe una situación previa habilitante, ya sea en forma de delito flagrante o hallazgo casual previo, que desencadene de forma lógica el posterior registro policial. Dicha lógica en el registro policial, una vez se accede de forma legítima, nos debe llevar, no obstante, a delimitar casos de extensión razonable y extensión irrazonable más allá de la estricta comprobación de lo atestiguado por el denunciante. Así, carecería de razonabilidad que la Policía, tras registrar el coche donde descubrió in fraganti al acusado en el momento de realizar el pase de papelina, realizara un registro domiciliario sin autorización policial. Parece lógico, pues, limitarse al espacio natural en el que se percibe el delito. Y, aun dentro de dicho espacio natural, debería limitarse la verificación y recogida de evidencias a las que sean de la misma naturaleza delictiva de las que legitimaron el acceso policial. on todo, podría alegarse que la actuación policial fue más allá de lo ordinariamente razonable, en tanto que se accedió a carpetas distintas a las que el testigo les había indicado. ¿Hasta dónde podía acceder la Policía en dicho registro? ¿Solo tenían que haber accedido a lo mínimamente indispensable a los efectos de estricta comprobación? Dicho de otro modo, no existiría duda alguna sobre la proporcionalidad de una intervención policial sobre el ordenador si la Policía solo se hubiera limitado a analizar el contenido de la carpeta "Mis documentos" pudiendo entenderse como la mínima actividad de

competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de 72 horas desde que fue ordenada la medida. Éstas injerencias policiales directas deberán ser examinadas con especial atención, dado que la multifuncionalidad de los datos que se albergan en estos dispositivos provoca una extrema debilidad de la tutela jurisdiccional del derecho del investigado a la reserva de su propio entorno virtual, pues una vez realizado el acceso al dispositivo, todos los datos, incluidos los relacionados con el secreto de las comunicaciones están al libre alcance del investigador[445].

---

investigación imprescindible para confirmar la verosimilitud de la denuncia. Sin embargo, la Policía fue más allá, debiéndose distinguir, a efectos analíticos, dos fases de acceso bien diferenciadas.
La sentencia del TC 173/2011, consideró que *nos encontramos ante uno de los supuestos excepcionados de la regla general, que permite nuestra jurisprudencia, pues existen y pueden constatarse razones para entender que la actuación de la policía era necesaria, resultando, además, la medida de investigación adoptada razonable en términos de proporcionalidad.* Razona la citada sentencia que *hay que tener en cuenta que la persona denunciada no estaba detenida cuando se practica la intervención, por lo que tampoco aparece como irrazonable intentar evitar la eventualidad de que mediante una conexión a distancia desde otra ubicación se procediese al borrado de los ficheros ilícitos de ese ordenador o que pudiera tener en la "nube" de Internet,* añadiendo que *también aparece como un interés digno de reseñar la conveniencia de que por parte de los funcionarios policiales se comprobara con la conveniente premura la posibilidad de que existiesen otros participes, máxime en este caso en que se utilizó una aplicación informática que permite el intercambio de archivos, o que, incluso, detrás del material pedófilo descubierto, pudieran esconderse unos abusos a menores que habrían de acreditarse.* La anterior conclusión del TC ha levantado críticas en sectores doctrinales, quienes entienden que en el caso abordado por la sentencia no concurría una urgencia y necesidad que legitimara la intervención policial. La propia sentencia del TC recibió un voto particular de la Magistrada Pérez Vera, quien no alcanza "a *entender por qué, estando el ordenador físicamente en poder de la Policía, las diligencias de investigación no podían esperar a que su realización contara con autorización judicial;* añadiendo que *el acceso a archivos de internet (como los que incriminaban al recurrente) sólo puede realizarse si el terminal en cuestión está conectado a la red, por lo que en nada se hubiera puesto en riesgo la labor investigadora de la Policía si, estando dicho terminal en su poder, se mantiene apagado hasta lograr la preceptiva autorización judicial".*

[445] CONDE-PUMPIDO TOURÓN, C. "La reforma procesal. Registro de sistemas informáticos (…) ob. cit. págs. 11 y 12. "*La inclusión de esta excepción por motivo de urgente necesidad pone de relieve un posicionamiento del legislador respecto a los derechos fundamentales en cuestión: se ha articulado una norma que recoge los pronunciamientos constitucionales respecto a la protección del derecho a la intimidad, pero estas previsiones se extienden a todo el contenido de los dispositivos, en que hay o puede haber datos relativos a comunicaciones. Si se trata de comunicaciones ya concluidas, como correos electrónicos o mensajería ya abiertos puede comprenderse la extensión, siempre dentro del principio de proporcionalidad. Pero pueden suscitarse problemas con los datos referentes a registros de llamadas, o mensajería no leída, que quizás exijan alguna limitación por vía jurisprudencial, por afectar al núcleo del derecho fundamental a secreto de las comunicaciones, cuya vulneración exige constitucionalmente autorización judicial".*

3.3.C) Contenido de la resolución judicial y práctica del registro.

La resolución del juez de instrucción que autorice el acceso a la información contenida en los dispositivos establece una serie de cautelas consecuencia del régimen privilegiado del "*derecho a la identidad virtual*[446], así deberá hacer mención a:

- los términos y el alcance del registro[447].
- Podrá autorizar la realización de copias de los datos informáticos.
- Fijará también las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación para hacer posible, en su caso, la práctica de un dictamen pericial (art. 588 sexies c LECrim)

En la práctica, para llevar a cabo el registro, tras el aseguramiento de la escena delictiva y la identificación de las fuentes de prueba, se precisa la intervención

[446] CONDE-PUMPIDO TOURÓN, C. "La reforma procesal. Registro de sistemas informáticos (…)". ob. cit. pág. 5. "*el Legislador otorga un tratamiento unitario a los datos contenidos en los ordenadores y teléfonos móviles, reveladores del perfil personal del investigado, configurando un derecho constitucional de nueva generación que es el derecho a la protección del propio entorno virtual*."

[447] RODRÍGUEZ LAÍNZ, J L. "¿Podría un juez español obligar a Apple a facilitar una puerta trasera para poder analizar información almacenada en un iPhone 6?". Diario La Ley nº 8729, marzo 2016, pág. 5 y 6. *"Uno de los principales problemas a los que se enfrentan las actuales técnicas forenses de análisis de información contenida en memoria de dispositivos de gran capacidad es precisamente la de delimitar el objeto de la injerencia a los contenidos que exclusivamente pudieran tener una relación directa con el objeto de la injerencia. Sería pecar de una ingenuidad extrema pensar que un terrorista va abrir una carpeta con el nombre de organigrama de la célula u objetivos objeto de vigilancia; por mucho que la STEDH (Sección 1ª) de 3 de julio de 2012 (caso Robathin c. Austria) considerara una situación de desproporción el análisis de todas las carpetas de un PC de abogado, y no su concreción a las abierta con el nombre de los dos clientes sospechosos de blanqueo de capitales. En un principio es probable que ni siquiera haya una idea clara de lo que se pretende buscar, la información relevante suele permanecer oculta en archivos de difícil hallazgo; como no sea examinándolos uno por uno, estableciendo enlaces o cruces de datos entre ellos, o incluso sometiéndolos a exámenes profundos en busca de archivos ocultos entre inofensivos documentos o fotografías. Pero cuando lo que se analiza es la memoria flash en busca de información borrada de forma intencionada por el usuario, o como consecuencia de operaciones automáticas, como quiera que el almacenamiento de datos se realiza por el sistema operativo sin criterios lógicos, la necesidad de acceder y analizar toda la información es inevitable. Las fotografías han de ser examinadas una a una, y respecto de los archivos de datos o documentos no cabría realizar otra discriminación que no fuera a través de sistemas de iltrado; que podrían ser eludidos con facilidad evitando palabras o datos comprometedores. Pero con tales antecedentes, y adoptándose las oportunas cautelas en orden a evitar en la medida de lo posible afectar a contenidos que realmente no tuvieran un interés aparente para la investigación, nada debería obstar a que se pudiera dictar una resolución motivada que habilitara a la policía a examinar el dispositivo".*

cualificada del personal técnico además del fedatario judicial -encargado de la preservación de la legalidad y de la custodia del material probatorio[448]-.

El clonado o volcado de datos del disco duro es[449] una garantía inicial de que lo que se copia es imagen fiel y exacta de lo que se ocupa, y debe vincularse a la obtención íntegra de la fuente de prueba, integridad vinculada en estas pericias informáticas especialmente al hecho de la modificabilidad y volatilidad mayor que en otras, por sus características, que va a servir objetivamente para garantizar la corrección de la información sobre la que versará después la pericia, y subjetivamente, para garantizar una defensa justa. La finalidad de esta operación es probable, por un lado, preservar la fuente original de prueba intacta e inmodifícada conforme sale del ordenador del investigado, razón por la que se acuerda su precinto quedando en poder del custodio de las pruebas judiciales, y por otro, permitir con la copia trabajar a los peritos informáticos sobre un elemento igual a la evidencia ocupada pero sin el riesgo de una alteración culposa o dolosa de su contenido, que lleve a conclusiones erróneas.

Es importante que el LAJ y los agentes policiales comisionados por el juez no olviden consignar, además de los datos a que se refiere el arto 569 LECrim., cuantos datos permitan identificar al usuario del ordenador tales como aprehensión de las claves de usuario y contraseñas que se descubran, apodos o *nicks* que se encuentren junto al ordenador, en caso de apertura *in situ* de archivos, directorios o carpetas, que no se escatime en datos técnicos como serían, por ejemplo, en los supuestos de pornografía infantil, la indicación del número y nombre de los archivos, el número de fotografías e

[448] En general, podrá realización *in situ* las capturas de pantalla sobre el que el LAJ dará fe, formando parte del contenido del acta, y cuya impresión puede adjuntarse para verificar los archivos obrantes con cargo al disco duro (art. 572 LECrim), procede realizar junto a ésta la aprehensión de los restantes archivos extraíbles en las distintas unidades de almacenamiento a analizar (en disquete, CD, DVD, USB, etc.) y, en su caso, proceder al volcado y clonado-copia de los mismos-, procurando inspeccionar sólo lo conducente a la investigación en curso, hacerlo sin perjudicar e importunar a los interesados más de lo necesario y sin comprometer su reputación y respetando los secretos que no interesen a la instrucción (art. 552 LECrim), debiendo devolver lo que no se relacione con la causa lo más inmediatamente posible.

[449] Para los casos en que la investigación descarte llevarse de la escena del delito los elementos que almacenan la memoria, o en los supuestos en que sea necesario realizar el análisis de su contenido con urgencia, los peritos procederán al clonado o volcado técnico del contenido del disco duro en una réplica con las copiadoras, con la práctica del oportuno resumen digital *hash,* y el secretario judicial garantizará la operación con su supervisión jurídica que, una vez finalizada, cerrará con el precinto del disco duro original, que quedará bajo su poder de custodia, para posibles futuros contrastes y/o contraperitajes, cediendo la copia clonada a los peritos para que, sobre ella, practiquen los oportunos análisis y pericias, sin riesgo de borrar o alterar la fuente original de prueba. Por lo tanto, el clonado o volcado del disco duro no es sino una operación.

imágenes encontrados, su impresión en soporte duradero y los megas de su capacidad y ocupación, etc.

En definitiva, las primeras diligencias de prevención llevadas a cabo por la Policía Judicial son esenciales, pudiendo llegar a condicionar todo el proceso judicial posterior. Si las primeras diligencias no se practican correctamente, pueden ser invalidadas total o parcialmente. En algunos casos, los defectos podrán corregirse o enmendarse en un momento procesal posterior, pero en otros no será posible tomar en consideración lo que se hubiera materializado en tales diligencias.

Salvo que constituyan el objeto o instrumento del delito o existan otras razones que lo justifiquen, se evitará la incautación de los soportes físicos que contengan los datos o archivos informáticos, cuando ello pueda causar un grave perjuicio a su titular o propietario y sea posible la obtención de una copia de ellos en condiciones que garanticen la autenticidad e integridad de los datos[450]. Por tanto, la aprehensión de los ordenadores, pantallas, impresoras, teclados y accesorios sólo procede si se trata de una ocupación de material a efectos de garantizar la pena de decomiso o para garantizar las oportunas responsabilidades civiles que puedan derivarse del ilícito investigado, y/o en su caso, si sobre ellas hubiera que realizar las correspondientes pericias.

En los casos de registros en la nube, la reforma se refiere también a los supuestos en los que la información se encuentra alojada en otros sistemas o en servidores disponibles en el *cloud computing* dadas las facilidades de almacenamiento que ofrece esa tecnología y la posibilidad del cliente o usuario de obtener la información en cualquier momento a través de su propio dispositivo informático[451].

[450] Artículo 588 sexies c. Apartado 2.

[451] RODRÍGUEZ LAÍNZ, J L. "Tres cuestiones polémicas sobre el registro de dispositivos electrónicos de almacenamiento masivo de información". Artículo monográfico, revista Sepín, septiembre de 2016. pág. 3 "*El almacenamiento en nube, por muy etéreo o abstracto que nos parezca, no es sino una forma más de alojamiento de datos externo en el que, a diferencia de los alojamientos físicos concretos propios de prestadores de servicios de alojamiento de datos, la determinación física del soporte electrónico que los alberga queda en buena parte difuminada. Lo importante para un alojamiento en la nube no es tanto la ubicación física de la información (que puede estar incluso distribuida entre múltiples alojamientos físicamente ubicados en localizaciones pertenecientes a distintos Estados, determinados de forma casi aleatoria), como su disponibilidad para el usuario en cuestión, cualquiera que sea el lugar en que se encuentre. El referente de su localización física pierde por ello peso frente a los únicos elementos determinantes accesibles de la identidad del usuario y del proveedor del servicio de alojamiento. Tanto en los alojamientos que pudiéramos definir como convencionales como en los alojamientos en la nube, lo primordial será la posibilidad de un acceso legítimo a través del dispositivo; lo cual, aparte del ejemplo*

Hay que resaltar que el registro de un sistema informático se ciñe normalmente a los límites físicos del lugar registrado. Mas una red informática tal vez no esté ubicada en un solo lugar, sino conectada con otras partes de la red mediante líneas de comunicación fijas o con conmutación. En estos casos se planteaba la cuestión de si es factible y lícito registrar los sistemas conectados cuando no estén situados en el lugar en que se realice el registro. Ello es importante, pues si el registro no es extenso, se corre el riesgo de que los datos sean borrados antes de que se pueda obtener otra orden de registro del lugar en el que estén situados físicamente, y, por el contrario, en las grandes redes, puede resultar prácticamente imposible establecer la ubicación física exacta de los datos[452].

El Convenio sobre ciberdelincuencia, en su art. 19, relativo al registro dispone que cuando se tengan motivos para creer que los datos buscados se hallan almacenados en otro sistema informático o en una parte del mismo situado en su territorio, y que dichos datos son legítimamente accesibles a partir del sistema inicial, puede extenderse el registro y ocupación a ese otro sistema. La consecuencia sería que el alcance del registro extenso se limitaría a las actividades que dicha persona estuviera autorizada a realizar en relación con el sistema conectado y sus datos, y que no se vulnerarían los derechos de esa persona más de lo permitido con ocasión del registro básico.

El art. 588 sexies c. 3 LECrim autoriza a quienes lleven a cabo el registro o tengan acceso al sistema de información o a una parte del mismo ampliarlo siempre que los datos sean lícitamente accesibles por medio del sistema inicial o estén disponibles para este. Esta ampliación del registro deberá ser autorizada por el juez, salvo que ya lo hubiera sido en la autorización inicial.

---

del consentimiento del interesado, puede tener lugar tanto cuando en el curso del registro se descubre un enlace o link que facilita un acceso directo a tales alojamientos como cuando se consiguen desvelar las claves de acceso a determinados perfiles de redes sociales, posiblemente relacionados con el objeto de la indagación. Obviamente, la utilización de una clave de usuario no es un baluarte inexpugnable que cierre el acceso a un registro legalmente autorizado".

[452] http://investigacioncriminal.info/2015/11/02/registro-remoto-sobre-equipos-informaticos-y-servidores/ a las 18.36 horas. No es la primera vez que se han podido ocultar pruebas de graves delitos económicos y de blanqueo de capitales relacionados con el crimen organizado a través de servidores web controlados telemáticamente con un simple teléfono móvil lo que ha permitido desconectarlos cuando son objeto de la ejecución de una entrada y registro ordenada por la autoridad judicial frustrándose la investigación por este motivo.

Resulta problemática la cuestión territorial en los registros en la nube. La posición en este punto del Convenio Europeo es la de un pleno sometimiento al criterio de soberanía; de sujeción a la ley nacional, y, por tanto, a la jurisdicción del Estado donde los datos se encuentren alojados[453]. La LECrim guarda silencio. Si partimos de la base de que tales alojamientos prácticamente no tienen una ubicación física definida, al ser esta de imposible o muy difícil determinación, nos encontraríamos con más referentes territoriales que el propio del dispositivo de comunicaciones sometido a un registro físico[454]. No cabría otra opción que la de excepcionar tal criterio de territorialidad a los alojamientos en la nube en aquellos supuestos en los que resulte imposible o especialmente gravoso indagar su localización física pues una ausencia de un criterio de territorialidad que permita la atribución de decisiones jurisdiccionales a un Estado concreto no puede poner al sujeto investigado en una mejor posición que cuando sí existe una localización geográfica concreta.

En los casos de urgencia, la Policía Judicial o el fiscal podrán llevar a cabo el registro inclusive en la nube, informando al juez inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, de la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de setenta y dos horas desde que fue ordenada la interceptación.

Se plantea la cuestión de si es más acertado que la policía por razones de urgencia practique directamente este registro en la nube o, si por el contrario, para estos

[453] RODRÍGUEZ LAÍNZ, J L. "Tres cuestiones polémicas sobre el registro de dispositivos (…)". ob. cit. pág. 4. De hecho, el mencionado art. 19.2 parte de la base de que tales datos objeto de extensión de un registro han de encontrarse almacenados "(...) en otro sistema informático o en una parte del mismo situado en su territorio (...)". El informe explicativo es aun más explícito, cuando de forma tan contundente descarta cualquier ambición expansionista de los Estados firmantes de basarse en la ubicación del enlace o punto de acceso a la fuente externa para legitimar una inmisión. De hecho, esta fue una de las cuestiones que más fueron objeto de discusión en los trabajos preparatorios; y que, ante la fortísima presión impuesta por Estados Unidos para un no reconocimiento de criterios de extraterritorialidad, terminó con la inclusión de tal cláusula. Como nos advierte el parágrafo 195 del Informe Explicativo, la norma no permite dirigir registros que superen las fronteras nacionales propias; debiendo acudirse en tales casos a los mecanismos convencionales de solicitud de cooperación judicial internacional

[454] RODRÍGUEZ LAÍNZ, J L. "Tres cuestiones polémicas sobre el registro de dispositivos (…)". ob. cit. pág. 4.*"(..)ubicado en el espacio jurisdiccional de una autoridad nacional; así como el del ámbito territorial del prestador del servicio a través del cual el sujeto investigado, o el dispositivo en cuestión, ha alojado la información objeto de indagación en la nube. El que una determinada información esté alojada en la nube no puede convertirse en una patente de corso de apatridia que la hiciera inmune a cualquier introspección hasta que se descubriera cuál es su ubicación física, única o plural"*.

supuestos es mejor solicitar la orden de conservación de datos del art. 588 octies, medida menos gravosa y garante de los derechos de las posibles personas afectadas. Será la urgencia de la actuación y el riesgo de manipulación o destrucción de la información la que hará decantarnos por una u otra norma[455]. En cualquier caso, la decisión de anticipar el acceso no tiene por qué suponer una merma de las garantías constitucionales que protegen a los ciudadanos de las actuaciones de aquellos. No hay que olvidar que la ulterior decisión del juez instructor abarca tanto a la oportunidad de la decisión de anticipación como a la debida valoración de los intereses constitucionales en conflicto. Así lo ha entendido la jurisprudencia del Tribunal Europeo de Derechos Humanos en la STEDH (Sección 4ª) de 12 de enero de 2016, caso *Szabó y Vissy* contra Hungría, aunque mostrándose especialmente exigente de que cualquier decisión de ratificación suponga una verdadera ponderación de los intereses constitucionales en conflicto, y no un simple placet o puesta en conocimiento[456].

Por último, en algunas ocasiones para abrir el ordenador y conocer su contenido puede ser necesario conocer la clave de usuario y contraseña que de ordinario bloquean el libre acceso al mismo, añadiendo un *plus* de protección a cualquier contenido protegido en su interior. Surge el interrogante de si se puede obligar al investigado a revelar sus claves y contraseñas *(login* y *password)* para investigar el contenido delictivo del ordenador, aunque la respuesta es negativa a tenor de los dispuesto en el artículo 588 sexies c en su apartado 5 LECrim[457]. Dispone el precepto que las

[455] RODRÍGUEZ LAÍNZ, J L. "Tres cuestiones polémicas sobre el registro de dispositivos (…)". ob. cit. pág. 6. Desde el mismo momento en que exista un riesgo cierto y elevado de destrucción o desaparición de la información mientras se emite y recibe por el destinatario la orden de retención, incluso por parte de este, sería absolutamente legítima la opción por la vía del acceso directo a tal información con posterior ratificación judicial, preferentemente

[456] RODRÍGUEZ LAÍNZ, J L. "Tres cuestiones polémicas sobre el registro de dispositivos (…)". ob. cit. pág. 6.

[457] RODRÍGUEZ LAÍNZ, J L. "Tres cuestiones polémicas sobre el registro de dispositivos (…)". ob. cit. pág. 7. El actual art. 588 sexies c) 5 tiene su origen en el art. 19.4 del CSC precepto referido al registro y confiscación de datos informáticos almacenados, que garantizaba la posibilidad de que las autoridades competentes pudieran ordenar a cualquier persona *"(...) que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite toda la información necesaria, dentro de lo razonable (...)", para permitir un registro de dispositivo de almacenamiento de datos o registrar información que pudiera obtenerse legítimamente a partir del sistema inicial o que fueran accesibles a partir de dicho sistema inicial.* El Convenio, que no reconocía la modalidad del registro remoto de equipos informáticos, ya definía este deber de colaboración como un deber de facilitación de información; en un sentido claramente relacionado con los conocimientos tanto técnicos –manejo del software, conocimiento de back-doors, técnicas de elusión o superación de medidas de seguridad o autenticación– como operacionales -desvelo de claves de acceso o de autenticación y ubicación de concretos datos o estructura de las bases de datos-; y establecía una

autoridades y agentes encargados de la investigación podrán ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite la información que resulte necesaria, siempre que de ello no derive una carga desproporcionada para el afectado, bajo apercibimiento de incurrir en delito de desobediencia[458]. Pero esta disposición no será aplicable al investigado o encausado, a las personas que están dispensadas de la obligación de declarar por razón de parentesco y a aquellas que, de conformidad con el artículo 416.2, no pueden declarar en virtud del secreto profesional.

Se trata de una facilitación de conocimientos, bien en forma de revelación de claves de acceso, si es que se conocen, bien de asesoramiento técnico, facilitando la información precisa para que puedan removerse las trabas o dificultades que impiden el acceso a la memoria del dispositivo[459].

El alcance del derecho de defensa determina que no pueda obligarse al investigado pues prevalece su derecho a no declarar contra sí mismo del artículo 520.2 b) LECrim, que deriva directamente del derecho constitucional previsto en el art. 24.2 CE. De ahí que la disposición del art. 588 sexies c, se aplique a quienes no tengan la calidad procesal de investigado o encausado, ni para aquellas que están dispensadas de declarar por razón de parentesco o exentas de declarar en virtud de secreto profesional.

Obviamente, la negativa del investigado u otros usuarios del ordenador a dar sus claves de acceso y contraseña no impide el uso de cualquier otra técnica que permita conocer el contenido de los archivos a registrar.

---

cláusula de proporcionalidad, razonabilidad, en la carga que habría de suponer para el sujeto obligado, no necesariamente operador de comunicaciones, fabricante, licenciatario del software o persona relacionada con el dispositivo objeto de registro: una salvaguardia frente a la imposición de un deber de colaboración especialmente gravoso.

[458] La noticia sobre la negativa de APPLE de facilitar al FBI los mecanismos para forzar la clave de acceso a un iPhone 5c de una presunta terrorista fallecida, plantea la cuestión de cómo exigir éste deber de colaboración a los fabricantes de dispositivos de comunicaciones buscando un equilibrio con los intereses de las compañías que se ven obligadas a invertir en tecnología para la privacidad de sus usuarios y a garantizar a ultranza esa privacidad. Finalmente, el FBI logró desbloquear el Iphone sin la ayuda de Apple y el Fiscal retiró los cargos contra la compañía, archivándose el asunto. No siempre esta colaboración es negativa así en la STS 587/2014, de 18 de julio, donde se trató de un supuesto de investigación criminal que contó con la colaboración de Apple en la facilitación de un software adecuado para permitir el examen de la información contenida en la memoria del iPhone 3 del sospechoso.

[459] RODRÍGUEZ LAÍNZ, J L. "¿Podría un juez español obligar a Apple a (…)". ob. cit. pág. 6.

Lo mismo es de aplicación al cifrado (que garantiza la autenticación, protege la confidencialidad e implica la utilización de un algoritmo de cifrado y una o más claves). El cifrado plantea el grave riesgo de que, sin la asistencia voluntaria del responsable del sistema o del titular, no se tenga acceso al sistema informático ni a los datos que se buscan. Por ello, al igual que en otras legislaciones se puede exigir a los responsables que permitan el acceso a los sistemas o a los datos, castigando el incumplimiento como desobediencia. No obstante, esas normas no pueden aplicarse cuando el propio operador de un sistema es también el sospechoso de haber cometido el delito, porque se violarían normas o principios constitucionales como el derecho a no confesarse culpable y a no autoincriminarse. Además pueden quedar exentas las personas que tengan otras razones legales para no cooperar, como las emparentadas con el sospechoso, o las que tengan la obligación profesional de guardar secretos (médicos, abogados,...).

3.4. Registro remoto sobre equipos informáticos.

En la investigación de los ciberdelitos, una de las diligencias más plausibles la constituye la posibilidad de acceder a un equipo informático mediante el registro remoto del mismo (art. 588 septies a, b y c LECrim)[460].

Esta nueva diligencia, que se encuentra presente en buena parte de las legislaciones[461], aunque no en el CSC, consiste en la utilización de programas que

[460] De hecho la conveniencia de incorporar el registro remoto de sistemas informáticos como instrumento en la lucha contra el terrorismo yihadista, ya se destacaba en la Memoria de la Fiscalía General del Estado de 2014, como herramienta legal imprescindible para facilitar la investigación de estas acciones en internet y en las redes sociales. Internet se ha convertido en el campo de entrenamiento virtual de los yihadistas y la herramienta perfecta para la comisión del ciberdelito consistente en reclutar, adoctrinar, formar y adiestrar a los terroristas y el medio para obtener financiación.

[461] VALVERDE MEGÍAS, R. Intervención de comunicaciones telemáticas y registro remoto. Ponencia presentada en el curso de Formación de Fiscales "Uso de las nuevas tecnologías y nuevas formas de delincuencia" que se celebró en el Centro de Estudios Jurídicos los días 27 al 28 de octubre de 2016. pág. 24. En Estados Unidos se tiene constancia de que el FBI ha venido utilizando este tipo de técnicas de investigación desde hace años. Así, poco después de que se hiciera pública la existencia del programa "Carnivore" como medio de intervención de las comunicaciones electrónicas de los investigados a finales de los 9012, el FBI desarrolló el programa "Magic Lantern", este sí un auténtico troyano que podía ser enviado por correo electrónico a los investigados y que instalaba en sus equipos infectados un programa de registro de pulsaciones (keylogger) que permitía averiguar las claves de cifrado de información en los equipos afectados. En 2007 fue el programa CIPAV, también del FBI, el que salió a la luz como

permiten de forma remota y telemática el examen a distancia del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o bases de datos. Obviamente, toda esta operación tiene lugar sin conocimiento de su titular o usuario, accediendo a la información del dispositivo electrónico que se controla a distancia mediante el empleo de un malware o virus informático[462].

Tradicionalmente el registro se realizaba *in situ*, pero en la actualidad la implantación de los denominados "programas espía", ya sean "registros de teclado" (*Keyloggers*), programas troyanos, o cualquier otro software o hardware que permita la apertura de una "puerta trasera" (*backdoor*), facilita el acceso de forma remota. A través de estos procedimientos se toma el control del dispositivo anfitrión, posibilitando el descubrimiento y captura de cualquier información alojada físicamente en él o, en su caso, virtualmente (en la nube) con ocasión de su acceso al repositorio correspondiente, o incluso la propia intervención de sus comunicaciones, obviando los problemas que podrían surgir a raíz de la utilización por el sujeto investigado de algún tipo de tecnología de seguridad o cifrado.

---

herramienta utilizada para la infección de equipos de investigados y la obtención por esta vía de información como el titular registrado del equipo informático, la dirección IP y MAC, puertos abiertos, sistema operativo, programas en funcionamiento, navegador, usuario activo o páginas web visitadas, para después enviar esa información a los servidores del FBI.

TEJERINA RODRÍGUEZ, O. *"El registro remoto de equipos informáticos" en http://www.internautas.org/html/8833.html* 16/11/2015 a las 17.43 horas.
Es preciso recordar que el Tribunal Constitucional de Alemania, anuló en Sentencia de 27 de febrero de 2008 la reforma de la Ley de los Servicios de Inteligencia del Estado Federal Nordrhein-Westfalen pues consideraba el registro remoto inconstitucional, aun limitándose a sospechosos de terrorismo, y se fijaba por primera vez el derecho al respeto y la integridad de sistemas informáticos. Según el Tribunal alemán aquella norma no cumplía ni la regulación del umbral de lesión, ni los requisitos procesales de los elementos de dicha lesión. No se cumplían los requisitos constitucionalmente exigibles de respeto a los derechos fundamentales que podrían verse lesionados con una medida de este tipo, y señaló que las medidas de vigilancia secretas realizadas por organismos estatales deben respetar un área central inviolable de la vida privada, porque el desarrollo de la personalidad en el área central de la vida privada incluye la posibilidad de expresar acontecimientos internos como percepciones y sentimientos, así como consideraciones, opiniones y experiencias de una naturaleza altamente personal, sin temer que organismos estatales puedan tener acceso a ello. Reconoció este Tribunal que en el caso de acceso secreto al sistema de tecnologías de la información del interesado, existe una necesidad de precauciones especiales establecidas por la ley que protegen el área central de la vida privada, y anuló las disposiciones impugnadas por quedar sobradamente acreditada una lesión del derecho general a la personalidad en su manifestación de la protección de la confidencialidad y de la integridad de tecnologías de la información. No obstante en octubre de 2011 fue revelado un troyano, cuya creación fue atribuida al Gobierno alemán capaz de analizar comunicaciones en curso, captar pulsaciones y generar capturas de pantalla.

[462] TEJERINA RODRÍGUEZ, O. "El registro remoto de equipos informáticos" *en http://www.internautas.org/html/8833.html* 16/11/2015 a las 17.43 horas.
El registro remoto de ordenadores se efectúa con los conocidos como "troyanos buenos".

Tanto la intromisión en el equipo, como la ausencia de conocimiento del titular del equipo informático, suponen una considerable injerencia en derechos fundamentales de la persona investigada, por lo que se han acotado con un listado *numerus clausus* los delitos que la pueden habilitar a la vez que se limita la duración temporal de dicho registro (art. 588 septies a y c).

A diferencia del registro de dispositivos regulado en el Capítulo VIII, el remoto no es un registro puntual, sino continuado en el tiempo. La medida servirá para conocer la información que almacene o transcurra por el sistema informático de manera continuada durante un tiempo determinado, por lo que suponen una afectación de elevada intensidad en los derechos a la intimidad, al secreto de las comunicaciones y, en general, al propio entorno virtual de la persona investigada. Estas consideraciones exigen la necesidad de un estricto control judicial, sin que sea posible su utilización por la Policía sin previa autorización jurisdiccional en casos de urgencia[463].

Es evidente que en la investigación del ciberdelito esta medida es de indudable utilidad para las Fuerzas de seguridad, ya que a través de esta nueva regulación la Policía Judicial podrá ser autorizada por los jueces de instrucción para la utilización de las claves de acceso a los sistemas informáticos que se pretenda investigar, o para instalar troyanos en los ordenadores de los investigados con la finalidad de recabar la información relevante que contengan, o la de otros equipos informáticos como tabletas y teléfonos inteligentes.

Instalado el correspondiente programa espía con orden judicial, o conseguido el acceso por claves, las posibilidades para la policía son infinitas, ya que no solo se puede acceder a la información que se almacena en el disco duro sino a toda la información obrante en el mismo.

[463] DELGADO MARTIN, J. "Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015". Diario La Ley nº 8693, Sección Doctrina, 2 de Febrero de 2016, pág. 11.

3.4. A) Presupuestos para su adopción.

Como ya se ha dicho, el intenso grado de injerencia que implica la adopción de esta medida justifica *per se* que se refuerce el ámbito objetivo de la misma acotándola a la investigación de un *numerus clausus* de delitos. Así, el artículo 588 septies a) LECrim en su apartado primero sostiene que "*El juez competente podrá autorizar la utilización de datos de identificación y códigos, así como la instalación de un software, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos,* siempre que persiga la investigación de alguno de los siguientes delitos[464]:

a) Delitos cometidos en el seno de organizaciones criminales.

b) Delitos de terrorismo.

c) Delitos cometidos contra menores o personas con capacidad modificada judicialmente.

d) Delitos contra la Constitución, de traición y relativos a la defensa nacional.

e) Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.

[464]VALVERDE MEGÍAS, R. "Intervención de comunicaciones telemáticas y registro remoto". ob. cit. pág. 28. Si se compara el ámbito de la intervención de las comunicaciones y el de los registros remotos, éste es un catálogo más cerrado porque el legislador ha considerado más limitativo de derechos el registro remoto:
- Desaparece la posibilidad de acordar la medida para la investigación de grupos criminales, restringiéndose exclusivamente a organizaciones criminales.
- Se mantiene la investigación de los delitos de terrorismo.
- La referencia a delitos dolosos con pena máxima de 3 o más años de prisión es sustituida por una lista cerrada de infracciones consideradas de especial gravedad, bien por el bien jurídico protegido (contra la Constitución, de traición y relativos a la defensa nacional) o por la vulnerabilidad de las víctimas (contra menores o personas con capacidad modificada judicialmente).
- Se mantiene la referencia a los delitos cometidos a través de TIC.

A pesar de su consideración de *numerus clausus,* con base en el primer y último supuesto (organización criminal y delitos cometidos con dispositivos tecnológicos) en la práctica puede resultar una medida de investigación cuya utilización resulte más frecuente de lo inicialmente previsto.

El último apartado no está exento de crítica[465], pues permite sin más los registros remotos para todo tipo de delitos cometidos a través de instrumentos informáticos, aunque faculta legalmente la utilización general de la medida en la investigación de los ciberdelitos. Se tendrá que estar a la proporcionalidad de la medida para determinar qué delitos de los que se cometen por medio de las TIC justifican el necesario sacrificio de los derechos de intimidad y secreto de las comunicaciones del investigado, por lo que debe ser interpretada de modo muy restrictivo, limitándose a ciberdelitos de especial gravedad[466].

El legislador tiene una mayor libertad de configuración sobre el derecho a la intimidad, y por ello no se plantea dudas de constitucionalidad en los casos de emergencia o riesgo de catástrofe o cuando la medida tenga por objeto la de localización de personas en situación de urgencia vital. Sin embargo, en otro tipo de casos, hay que tener en cuenta que esta medida afecta no solo a datos concretos concernientes al sospechoso, sino en general al examen a distancia y sin conocimiento de su titular o usuario de la totalidad del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos o base de datos, lo que explica, por una parte, la sujeción de la medida a los principios generales en materia de

[465] TEJERINA RODRÍGUEZ, O. "*El registro remoto de equipos informáticos" en* http://www.internautas.org/html/8833.html 16/11/2015 a las 17.43 horas. Considera inconstitucional este último inciso pues sostiene "*para cualquier Estado de Derecho, es increíble que además se establezca de una manera tan vaga, sin precisiones de ningún tipo, y creando una inseguridad jurídica absoluta sobre los supuestos de hecho en que se podrán utilizar. Entendemos que es a todas luces inconstitucional, porque no contiene justificación de proporcionalidad ni concreción alguna de su finalidad (solo dice descubrir delitos en Internet), en respeto de los derechos fundamentales que así quedarán conculcados. Cualquier prueba así obtenida, la ordene o no un juez, no puede tener cabida en un proceso penal justo que quiera respetar las garantías de la debida tutela judicial efectiva".*

[466] CONDE-PUMPIDO TOURÓN, C. "La reforma procesal. Registro de sistemas informáticos …". ob. cit. pág. 21

restricción de los derechos consagrados en el artículo 18 CE, y por otra, que quede reservada a delitos de especial gravedad[467].

Dado el nivel de injerencia en los derechos fundamentales, la LECrim (art. 588 septies a apt. 2º) establece que la *"resolución judicial que autorice el registro deberá especificar*:

a) los ordenadores, dispositivos electrónicos o sistemas informáticos o parte de los mismos, medios informáticos de almacenamiento de datos o bases de datos, datos u otros contenidos digitales objeto de la medida[468].

b) El alcance de la misma, la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el software mediante el que se ejecutará el control de la información.

c) Los agentes autorizados para la ejecución de la medida.

d) La autorización, en su caso, para la realización y conservación de copias de los datos informáticos.

e) Las medidas precisas para la preservación de la integridad de los datos almacenados, así como para la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso.

La Ley no se refiere expresamente a límites geográficos, pero por el límite de territorialidad de la jurisdicción ha de entenderse que el dispositivo al cual se introduce el malware para su registro remoto ha de estar ubicado en España. Si el sistema investigado se encuentra ubicado físicamente fuera del territorio del Estado

[467] TEJERINA RODRÍGUEZ, O. "*El registro remoto de equipos informáticos" en http://www.internautas.org/html/8833.html* 16/11/2015 a las 17.43 horas.

[468] VALVERDE MEGÍAS, R. Intervención de comunicaciones telemáticas y registro remoto (…) ob. cit. pág. 29. Se trata de una relación suficientemente amplia como para dar cabida a cualquier dispositivo apto para generar, recibir, transmitir o almacenar datos digitales de cualquier tipo. Por lo tanto, quedarán comprendidos en este listado:
- Ordenadores de cualquier tipo, fijos o portátiles, desde personales a grandes servidores informáticos de proveedores de servicios en internet, llegado el caso.
- Tablets y smartphones.
- Dispositivos autónomos de mero almacenamiento tales discos duros externos, dispositivos de memoria flash (tarjetas, pendrives,...) o unidades ópticas (discos).

investigador, aunque técnicamente sea posible la penetración en los dispositivos cualquiera que sea su ubicación, sería necesario acudir a la correspondiente comisión rogatoria o al mecanismo de cooperación que corresponda de acuerdo con los tratados[469].

Por último, al igual que sucede en el registro de dispositivos electrónicos, se prevé la posibilidad de que el registro se amplíe a datos almacenados en una red informática privada o en "*la nube*". Así, cuando los agentes que lleven a cabo el registro remoto tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del mismo, pondrán este hecho en conocimiento del juez, quien podrá autorizar una ampliación de los términos del registro (art. 588 septies a apt. 3). Pero en este caso, siempre será necesaria la autorización judicial previa, pues no se permite el desarrollo de la medida por la Policía Judicial con un control a posteriori como sucede en el registro de dispositivos[470].

---

[469] VALVERDE MEGÍAS, R. "Intervención de comunicaciones telemáticas y registro remote (…)". ob. cit. pág. 30 y 31. Esta cuestión ha sido objeto de debate acerca de si puede derivarse algún conflicto de jurisdicción como consecuencia de registrar esas bases de datos ubicadas fuera del territorio nacional sin acudir a instrumentos de cooperación internacional con el estado en que los servidores de la empresa se ubican.
Más allá de cuestiones prácticas como la demora en la tramitación de la instrucción con la consiguiente pérdida de información, o aún más grave, la imposibilidad de recabar cooperación internacional de determinados países, que generaría el indeseable efecto de que los delincuentes busquen servicios web en esos mismos países para abortar cualquier posible investigación sobre ellos, entendemos que debe rechazarse la objeción de falta de jurisdicción:
Cuando el investigado accede desde su ordenador (o lo hace la policía desde ese equipo en el curso de un registro) a estos servicios, el mismo en ningún momento se está desplazando a otro país a consultar su información: es la información la que pasa al ordenador del investigado, aun en modo temporal, de manera que durante el tiempo en que está consultándola podemos afirmar que esa información está en su equipo.
Este conflicto se dejaba entrever en el Proyecto de Código Procesal Penal, que indicaba en su art. 350.4 que "El registro remoto sólo podrá ser autorizado cuando los datos se encuentren almacenados en un sistema informático o en una parte del mismo situado en territorio sobre el que se extienda la jurisdicción española. En otro caso, se instarán las medidas de cooperación judicial internacional en los términos establecidos por la Ley, los Tratados y Convenios internacionales aplicables y el derecho de la Unión Europea".
Sobre este precepto cabía afirmar que en el almacenamiento virtual en forma de estructura servidor-cliente (siendo el "servidor" el sistema informático de almacenamiento y el "cliente" el sistema informático del usuario que estaría en España) estamos en realidad ante un sistema complejo parte del cual (la parte del cliente) estaría en territorio nacional.
El hecho de que toda referencia al respecto de la ubicación de los sistemas haya desaparecido en la reforma introducida por la LO 13/2015 pese a que la regulación actual del registro remoto provenga directamente de aquélla, permite pensar que el legislador ha descartado el conflicto en este punto, asumiendo simplemente que lo que puede verse en España está en España.

[470] Se plantea la posibilidad de que el juez de instrucción español intervenga los correos electrónicos almacenados en un servidor extranjero, sin necesidad de emitir una comisión rogatoria. En el Anteproyecto de LECrim de 2013 se establecía que "El registro remoto –de equipos informáticos- sólo

Respecto a este registro remoto en la nube, sin perjuicio de que el sujeto investigado utilice habitualmente el mismo equipo y éste pueda ser monitorizado mediante alguno de los programas espía en los términos que acabamos de relatar, una segunda vía de acceso puede encontrarse en la obtención de las correspondientes claves al prestador del servicio de "*cloud computing*" (*Dropbox*, *Google Drive* de Google, *iCloud* de Apple, *OneDrive* de Microsoft, etc.), con lo que perdería relevancia la identificación del dispositivo o sistema utilizado por el investigado[471].

3.4.B) Duración y deber de colaboración.

Otro límite que establece la ley para mitigar la injerencia de esta diligencia de investigación tecnológica es el de su duración temporal: un mes prorrogable como máximo por iguales periodos de tiempo hasta los tres meses (art. 588 septies c LECrim).

La complejidad para efectuar el registro remoto ha dado lugar a que el legislador desarrolle (en el art. 588 septies b LECrim) un deber de colaboración ampliado respecto a otras diligencias de investigación tecnológicas. Así, resultan afectados por esta disposición:

- Por remisión al art. 588 ter e: *a)* los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información; y *b)* toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual.

---

podrá ser autorizado cuando los datos se encuentren almacenados en un sistema informático o en una parte del mismo situado en territorio sobre el que se extienda la jurisdicción española. En otro caso, se instarán las medidas de cooperación judicial internacional en los términos establecidos por la Ley, los Tratados y Convenios internacionales aplicables y el derecho de la Unión Europea" (art. 350.4). La LECrim guarda silencio a este respecto. No obstante, el art. 2.4 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y del correo electrónico, impone el sometimiento a la ley nacional de todos los prestadores que operen en territorio nacional en base a criterios de establecimiento jurídico o de medios de producción relevantes.

[471] CABEZUDO RODRÍGUEZ, N. "Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal". ob. cit. págs. 7 a 60.

- Además, el art. 588 septies b LECrim incluye a los titulares o responsables del sistema informático o base de datos objeto del registro, así como a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos (exceptuados el investigado, los parientes dispensados de la obligación de declarar y los amparados por secreto profesional).

El deber de colaboración establecido, so pena de incurrir en delito de desobediencia, y además del deber de guardar secreto, comprenderá: *a)* la colaboración precisa para la práctica de la medida y el acceso al sistema; *b)* la asistencia necesaria para que los datos e información recogidos puedan ser objeto de examen y visualización; *c)* la persona "que conozca el funcionamiento o las medidas", que facilite la información que resulte necesaria.

Se trata de un deber configurado en términos muy amplios que permite incluso acudir a los denominados hackers para que colaboren en la adopción y práctica de esta medida.

Al hilo del deber de colaboración debe tenerse en cuenta el papel que habrán de jugar en la puesta en práctica del registro remoto las empresas desarrolladoras de antivirus, puesto que constituyen una de las barreras técnicas que deberán ser superadas por la investigación para lograr la instalación de un programa que permita el acceso remoto. Por tanto, el éxito en la práctica de la diligencia del registro remoto pasará bien por desarrollar un programa que no pueda ser detectado por el sistema de seguridad que tuviera instalado el dispositivo objeto de control, o bien, por lograr la colaboración de la empresa desarrolladora de ese sistema de seguridad, siendo dicha colaboración la que tendría cabida en las previsiones del art. 588 septies b LECrim[472].

[472] VALVERDE MEGÍAS, R. "Intervención de comunicaciones telemáticas y registro remoto". ob. cit. pág. 37. "*A pesar de la previsión legal, lograr la colaboración de las empresas de seguridad informática para que proporcionen vías de acceso o descubran a la policía las vulnerabilidades de sus propios sistemas de seguridad es harto complicada: 1) Se tratará frecuentemente de empresas situadas fuera del ámbito jurisdiccional español, por lo que no estarán sujetas a la legislación o el poder coercitivo del sistema judicial español. 2) Desde el punto de vista reputacional, resultaría catastrófico que se filtrase que la empresa de seguridad ha dejado deliberadamente vulnerabilidades en sus sistemas para permitir el acceso policial a los sistemas informáticos teóricamente protegidos. 3) Las mismas vulnerabilidades propiciadas o comunicadas a la policía son vulnerabilidades susceptibles de ser usadas maliciosamente por cualquier malware que no dependa de la actividad policial o judicial, puesto que la brecha de seguridad no distinguirá entre accesos lícitos e ilícitos".*

3.5 El agente encubierto informático.

La figura del agente encubierto contenida en el artículo 282 bis LECrim, fue introducida mediante LO 5/1999, de 13 de enero, *de modificación de la Ley de Enjuiciamiento Criminal en materia de perfeccionamiento de la acción investigadora relacionada con el tráfico ilegal de drogas y otras actividades ilícitas graves*[473].

En esencia, la figura del agente encubierto permite, en las investigaciones que afectan a actividades propias de la delincuencia organizada, autorizar a funcionarios policiales para actuar bajo identidad supuesta.

Mediante dicha autorización judicial, toda la información que vaya obteniendo el agente encubierto deberá ser puesta a la mayor brevedad posible en conocimiento de quien autorizó la investigación y aportarse al proceso en su integridad.

Con esta misma idea, se vino considerando desde hacia tiempo la conveniencia de potenciar las posibilidades de utilización del agente encubierto en las investigaciones *on-line*, precisamente por las posibilidades que el uso de esta técnica ofrece para el esclarecimiento de los hechos ilícitos que se cometen a través de la red y para la determinación de sus autores y poder luchar contra la delincuencia a través de internet, en supuestos como podrían ser la captación, e incluso las comunicaciones entre terroristas[474], las estafas informáticas masivas concertadas por grupo organizado (phishing), la distribución grupal de pornografía infantil, o cualesquiera otros delitos

[473]Esta figura ha suscitado diversos problemas derivados de la pluralidad de situaciones a las que puede verse abocado el agente encubierto en el curso de la investigación criminal, muchas de ellas imprevisibles y que, por tanto, no pueden ser valoradas y amparadas previamente por la resolución judicial habilitante de la infiltración policial. La valoración sobre la proporcionalidad de las actuaciones con entidad jurídico-penal realizadas en el ámbito de la infiltración en relación con la finalidad de la investigación, queda sujeta a un juicio "a posteriori" realizado por el órgano competente para el enjuiciamiento de aquellas, lo que genera una situación de inseguridad jurídica para el agente encubierto.

[474] Los terroristas que organizaron el atentado en París en noviembre de 2015, se comunicaron a través de juegos *on-line* de la PSP4. http://www.elperiodico.com/es/noticias/internacional/terroristas-atentado-paris-emplean-playstation-para-comunicarse-4674944

convencionales de organización, vehiculizados a través de las nuevas tecnologías (ejem, venta de droga por internet, blanqueo informático de capitales, etc.)[475].

Ello se llevó a cabo en la reforma procesal por Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, donde se menciona esta figura al considerar en el preámbulo que *"resulta ocioso explicar la importancia del denominado agente encubierto a efectos de la persecución de determinadas modalidades delictivas. Pues bien, íntimamente relacionado con las anteriores medidas de investigación tecnológica, la reforma actualiza el uso de tales recursos por el agente encubierto en las tareas que tiene encomendadas. En concreto, de una parte se prevé la posibilidad de que los agentes encubiertos puedan obtener imágenes y grabar conversaciones, siempre que recaben específicamente una autorización judicial para ello; y de otra, se regula la figura del agente encubierto informático, que requiere autorización judicial para actuar en canales cerrados de comunicación (puesto que en los canales abiertos, por su propia naturaleza, no es necesaria) y que a su vez, requerirá una autorización especial (sea en la misma resolución judicial, con motivación separada y suficiente, sea en otra distinta) para intercambiar o enviar archivos ilícitos por razón de su contenido en el curso de una investigación"*.

Al respecto se añadieron dos nuevos apartados 6 y 7 al artículo 282 bis con la siguiente redacción: *"6. El juez de instrucción podrá autorizar a funcionarios de la Policía Judicial para actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación con el fin de esclarecer alguno de los delitos a los que se refiere el apartado 4 de este artículo o cualquier delito de los previstos en el artículo 588 ter a. El agente encubierto informático, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos. 7. En el curso de una investigación llevada a cabo mediante agente encubierto, el juez competente podrá autorizar la obtención de imágenes y la grabación de las conversaciones que puedan mantenerse en los encuentros previstos*

[475] VELASCO NÚÑEZ, E. "Delitos cometidos a través de Internet (…)". ob. cit. pág. 207.

entre el agente y el investigado, aun cuando se desarrollen en el interior de un domicilio."

Estas nuevas disposiciones regulan la novísima figura de los *"agentes encubiertos informáticos"*, una suerte de "espías" lícitos en la red, que ya habían sido aceptados por la Jurisprudencia, y que permiten a la Policía Judicial a través del uso de identidades falsas, infiltarse en redes sociales e intercambiar archivos ilícitos en internet en el transcurso de una investigación para identificar a los presuntos delincuentes.

La LECrim da cobertura a la actuación del agente encubierto infiltrado mediante identidad supuesta en canales de comunicación, es decir, en las denominadas redes sociales de internet. Pero ha de tratarse de canales cerrados de comunicación. Significa por tanto, que la autorización judicial se requiere para la navegación en canales cerrados, y no canales o foros abiertos donde los agentes policiales pueden utilizar una identidad supuesta en el ejercicio de las funciones que legalmente les corresponden de prevención e investigación del delito a que se refieren los arts. 11 de la LO de Fuerzas y Cuerpos de Seguridad y 282 LECrim.

Existe, por tanto, un marco de actuación policial inicial en la web que puede realizarse sin necesidad de una previa autorización judicial del agente encubierto virtual o informático[476]:

A) El *ciber-patrullaje*, o actuación destinada a la vigilancia, prevención y evitación de ilícitos cuya evidencia conste en la red, que tiene lugar en fuentes abiertas en la web o canales no cerrados de comunicación. Los denominados rastreos policiales que se efectúan en espacios de libre acceso como las redes P2P o en determinados ámbitos de las redes sociales o en general en foros abiertos de internet. Es una técnica policial perfectamente válida y en la que no son exigibles requisitos especiales.

El acceso a internet y a los rastros que el delincuente deja en él, no afecta a derechos fundamentales, pues ni es privado ni íntimo lo que se deja allí, ni se trata de una telecomunicación formalmente protegida cuyo secreto deba guardarse, ni son datos

[476] Conclusiones de la II jornada sobre el marco jurídico de actuación del agente encubierto (Madrid, 29 de mayo de 2015). Ministerio de Justicia.

protegidos automatizadamente los que se realizan al colgar en internet ofertas, más o menos camufladas de objetos de circulación delictiva.

En los delitos en los que se expone el contenido ilícito (ej. venta de droga, reclutamiento de terroristas, intercambio de pornografía infantil…) utilizando internet como medio de difusión hay un claro propósito previo del investigado a delinquir, exteriorizado al dirigirse a un círculo más o menos amplio y generalmente anónimo de presuntos destinatarios desconocidos, de cuya actuación precisa para materializarse y consumarse la acción. La oferta supone la cesión anónima a todos sus presuntos aceptantes de los datos que se expongan al hacerlo, que obviamente, si se llevan a los cuerpos policiales o al juez, no vulneran el derecho recogido en el art. 18.4 CE, pues ni se hallan tratados automatizadamente por el mero hecho de aparecer en internet, ni se ceden ilícitamente si se consiguen en ese escaparate abierto al acceso de cualquier usuario que es la red[477].

Es de frecuente utilización en las investigaciones policiales en la red el uso procedimientos mecánicos[478]. Es decir, utilización de sistemas de rastreo que debidamente programados y a partir de voces o de conceptos realizan búsquedas en foros abiertos. Se trata también de una concreta ejecución de las funciones de prevención del delito a que se refiere el artículo 11 de la Ley de Fuerzas y Cuerpos de Seguridad o de las que corresponden a la policía judicial a tenor de lo establecido en el artículo 282 de la LECrim[479].

---

[477] http://investigacioncriminal.info/2015/10/31/el-agente-policial-virtual-encubierto-una-nueva-medida-procesal-para-perseguir-el-crimen-organizado/.

[478] El programa denominado "Quijote" creado por alumnos de la Cátedra Amaranto de Seguridad Digital e Internet del Futuro. La herramienta está diseñada para la localización de los usuarios que comparten material pedófilo.
El "Quijote" centra su búsqueda en redes Peer to Peer (P2P) y en archivos multimedia, es decir, fotografías o videos. Esta búsqueda la realiza en base a una secuencia única que poseen todos los ficheros que se comparten en internet. El programa rastrea esa secuencia y detecta, en todo internet, el ordenador que contiene ese archivo. Además, permite hacer búsquedas selectivas por direcciones IP, por provincias, ciudades, países, incluso por usuarios.

[479] ZARAGOZA TEJADA, J. I. "La reforma operada por Ley 13/2015. El Agente Encubierto Informático". Ponencia presentada en el curso de Formación de Fiscales "Uso de las nuevas tecnologías y nuevas formas de delincuencia" que se celebró en el Centro de Estudios Jurídicos los días 27 al 28 de octubre de 2016. pág. 8. *"Son por ejemplo muy característicos la utilización de metabuscadores específicamente preparados para la localización de archivos pornográficos. Los metabuscadores son herramientas específicamente diseñadas para localizar contenidos pornográficos a partir del hash de archivos ya localizados e identificados como pornográficos o a partir de otros datos identificativos*

En relación con este *ciber-patrullaje* o rastreo policial ha tenido oportunidad de pronunciarse en múltiples ocasiones nuestro Tribunal Supremo[480].

B) La ocultación de la condición de policía, haciéndose pasar por un usuario más de la red, sin perjuicio de la necesidad de autorización judicial para amparar ulteriores contactos con la persona investigada, especialmente en los supuestos en que tienen lugar a instancia del agente policial[481] .

Algunas sentencias de la Sala Segunda del Tribunal Supremo habían dado por buena esta posibilidad sin exigir para ello autorización judicial como la STS 767/2007, de 3 de octubre, que se pronuncia sobre un supuesto en el que el uso del *nickname* se llevó a efecto en espacios públicos y en funciones generales de prevención de la delincuencia[482]. Considera, por tanto, nuestro Alto Tribunal que la utilización del

---

(nombres de archivos; fotografías etc...). La localización de archivos que están siendo difundidos a través de la red permite seguir el movimiento de los mismos y en definitiva conocer la IP de origen o de destino de la transmisión de contenido y, en consecuencia, la identidad de aquellos que han intervenido en la actividad delictiva aunque para conocer el titular de esa IP, ya sí será necesario autorización judicial."

[480] La STS 236/2008, de 9 de mayo, señalaba que "*los rastreos que realiza el equipo de delitos telemáticos de la Guardia Civil en internet tienen por objeto desenmascarar la identidad críptica de los IPS (Internet protocols) que habían accedido a los "hash" que contenían pornografía infantil. El acceso a dicha información, calificada de ilegítima o irregular, puede efectuarla cualquier usuario. No se precisa de autorización judicial para conseguir lo que es público y el propio usuario de la red es quien lo ha introducido en la misma"*.
La STS 292/2008, de 28 de mayo, que señalaba: *"Ahora bien, cuando la comunicación a través de la Red se establece mediante un programa P2P, como en el EMULE o EDONKEY, al que puede acceder cualquier usuario de aquélla, el operador asume que muchos de los datos que incorpora a la red pasen a ser de público conocimiento para cualquier usuario"*.

[481] STS 752/2010, de 14 de julio, afirma que "*es cierto que la agente actuó de forma encubierta, haciéndose pasar por un usuario más de la red, pero ello no infringe ningún derecho del acusado en cuanto se limitó a seguir el contacto iniciado por el mismo, que incluyó el envío de las imágenes unidas a las actuaciones, luego se trataba de una actividad de investigación policial lícita*".

[482] La STS 767/2007, de 3 de octubre, considera correctas las actuaciones iniciales del agente policial razonando que *"efectivamente, lo cierto es que los agentes de la autoridad, cuando realizan las labores habituales de vigilancia para prevenir la delincuencia informática tuvieron noticia casual de la existencia de un posible delito de difusión de pornografía infantil. Realizaron las investigaciones oportunas y, sólo cuando tuvieron la convicción de estar efectivamente en presencia de hechos presuntamente delictivos, confeccionaron el oportuno atestado que remitieron a la Fiscalía de la Audiencia Provincial donde se instruyeron las pertinentes diligencias informativas y, acto seguido, tras la denuncia en el Juzgado de Instrucción, las Diligencias Previas. Tal método de proceder es absolutamente correcto y ninguna objeción puede merecer"*.

La STS 752/2010, de 14 de julio, afirma que en relación con la vulneración del derecho al secreto de las comunicaciones, no aporta dato alguno fuera de identificarla con la captación de los mensajes y contactos realizados por el mismo a través de internet, olvidando que el acceso a la información así producida puede efectuarla cualquier usuario, no precisándose autorización judicial para conseguir lo que es público

agente encubierto no excluye la posibilidad de que, con carácter previo al uso de esta figura, los agentes de las Fuerzas y Cuerpos de seguridad del Estado puedan realizar una investigación previa que implique tomar contacto con alguno o algunos de los investigados a fin de reunir elementos indiciarios suficientes que permitan abrir una investigación judicial más definida[483]. Pero si en el curso de su investigación se revelara necesario infiltrarse en canales cerrados de comunicación en internet, la incursión en dichos foros implicaría necesariamente una intromisión en el derecho al secreto de comunicaciones respecto a quienes son parte en ese foro privado y, consecuentemente, sería necesaria la resolución judicial a la que se refiere el artículo 282bis 6 de la Ley de Enjuiciamiento Criminal.

El ámbito objetivo de aplicación de esta técnica policial, es el de los delitos previstos en el apartado 4 del artículo 282 bis 4 y los delitos relacionados en el artículo 588 ter LECrim.

Limitar las posibilidades de uso de esta figura a la investigación de actividades de delincuencia organizada (art. 282 bis apt. 4), cuyo objeto es uno de los tipos delictivos que se relacionan en el propio precepto con carácter de *númerus clausus*, restringía considerablemente las posibilidades de utilización de esta técnica en las investigaciones *on line*. Muchas de las actividades ilícitas más frecuentes -como el acoso a menores de edad- no se llevan a efecto en el marco de grupos de delincuencia organizada, y otras de ellas -como los ataques a sistemas informáticos- no están incluidas en la mencionada relación de delitos. Ello queda solventado con la aplicación de esta técnica también para los delitos relacionados en el artículo 588 ter a), entre los

cuando el propio usuario de la red ha introducido dicha información en la misma (*vid.* STS 739/2008 y las citadas en la misma)".

[483] Un pronunciamiento similar, se dio en las SSTS 277/2016 de 6 de abril, 835/2013, de 6 de noviembre, *"carecería de sentido, con el fin de sostener la validez de la diligencia de prueba, la exigencia de que la autorización del agente encubierto se produzca a ciegas, con exclusión de cualquier contacto previo entre la persona que va a infiltrarse en la organización y quienes aparecen como miembros sospechosos de una red delictiva. (...) Es contrario a elementales máximas de la experiencia concebir la infiltración en un grupo criminal como la respuesta a una invitación formal a un tercero que, de forma inesperada, curiosea entre los preparativos de una gran operación delictiva. La autorización judicial, por si sola, no abre ninguna puerta al entramado delictivo que quiere ser objeto de investigación...De ahí que la resolución judicial (de habilitación del agente encubierto) tiene que producirse en el momento adecuado que, como es lógico, no tiene porque ser ajeno a una relación previa que contribuya a asentar los lazos de confianza (...) que un funcionario policial lleve a cabo tareas de investigación antes de llegar a tener el carácter que regula el artículo 282 bis no implica que no pueda servir válidamente como testigo respecto a lo visto y oído en tiempo anterior*".

que se incluyen los delitos del artículo 579.1 LECrim (*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)* y los delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación[484].

El ámbito subjetivo de esta medida. Sólo podrán actuar como agentes encubiertos los funcionarios de la Policía Judicial, entendiendo por tales aquellos miembros de cuerpos policiales que conforme a la Ley Orgánica 2/1986 del 13 de marzo sobre Fuerzas y Cuerpos de Seguridad, y demás leyes en vigor, ostenten funciones de investigación respecto a los hechos delictivos comprendidos en el ámbito objetivo de la aplicación de la Ley[485].

En ocasiones, en el marco de actuaciones de investigación realizadas sobre delitos de narcotráfico y de terrorismo, se ha planteado la posibilidad de si agentes policiales extranjeros podrían actuar como agentes encubiertos en territorio español. Aun cuando el artículo 282bis de la LECrim requiere que se trate de un funcionario de la Policía Judicial española, resulta obvio que esta exigencia solo es predicable cuando el órgano autorizante es, precisamente, un órgano judicial español. Sin embargo, en opinión de algunos autores, resulta perfectamente posible la actuación en territorio español de agentes encubiertos pertenecientes a las fuerzas y cuerpos de seguridad de otro estado, siempre y cuando hayan sido preceptivamente autorizados por los órganos judiciales del estado correspondiente si bien su actuación, claro está, deberá sujetarse a

[484] ZARAGOZA TEJADA, J. I. "La reforma operada por Ley 13/2015. El Agente Encubierto Informático".ob. cit. pág. 23.*"En definitiva, se flexibiliza la posibilidad de uso de esta figura en supuestos en los que no concurra delincuencia organizada, sin perjuicio de la aplicación de los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad a los que se hace expresa referencia en el artículo 588bis a) de la LECrim. Pues una interpretación excesivamente axiológica y conjunta de ambos preceptos permitiría inferir que podría autorizarse este tipo de medidas para la investigación de cualquier delito cometido a través de las nuevas tecnologías y dar cabida la utilización del agente encubierto en investigación de delitos de poca gravedad o con poca trascendencia social como delitos leves de estafa o coacciones cometidas a través de las redes sociales, lo que resultaría absolutamente desproporcionado dado los derechos e intereses en juego".*

[485] En cuanto a las Policías Autónomas del País Vasco y Cataluña habrá que estar no sólo a lo dispuesto en la Ley Orgánica 2/1986 sino también en sus respectivos Estatutos de Autonomía. Parece claro que no podrán actuar de esta manera los Cuerpos de Policía Local, pues además de su carácter exclusivamente colaborador no están autorizados para desarrollar investigaciones de hechos delictivos, salvo las diligencias de prevención y la instrucción de atestados por accidentes de circulación (artículo 53 de la Ley Orgánica 2/1986).

las reglas y procedimientos de nuestro estado en tanto en cuanto dicha actuación de investigación sea desarrollada en nuestro territorio nacional[486].

El agente encubierto, una vez obtenida la preceptiva resolución judicial, estará habilitado para realizar cualquier acto de investigación sin necesidad de exigirse una nueva resolución judicial habilitadora para ello salvo que, claro está, dicho nuevo acto de investigación conlleve una intromisión en el contenido esencial del algún derecho fundamental como es el derecho al secreto de comunicaciones, intimidad o inviolabilidad del domicilio. De tal modo que habilitado ya el agente encubierto *on-line* para actuar en foros privados de comunicación, si en el curso de dicha investigación se hace necesario realizar algún tipo de acto (aunque sea en el mundo físico) que no conlleve la limitación de un nuevo derecho fundamental no sería necesario una nueva resolución judicial adicional[487].

[486] Convenio Europeo de Asistencia Judicial Penal del 29 de mayo del 2000 en su artículo 14, regula las investigaciones encubiertas de la siguiente manera: "*El Estado miembro requirente y el Estado miembro requerido podrán convenir en colaborar para la realización de investigaciones de actividades delictivas por parte de agentes que actúen infiltrados con una identidad falsa. 2. La decisión sobre la solicitud la tomaran en cada caso las autoridades competentes del Estado miembro requerido atendiéndose a su derecho interno y a los procedimientos nacionales. Los Estados miembros acordarán la duración de la investigación encubierta, las condiciones concretas y el régimen jurídico de los agentes de que se trate, ateniéndose a sus respectivos derechos internos y procedimientos nacionales. 3. Las investigaciones encubiertas se realizaran de conformidad con el derecho y los procedimientos del Estado miembro en cuyo territorio se realicen. Los Estados miembros interesados colaborarán para garantizar la preparación y supervisión de la investigación encubierta y la adopción de medidas para la seguridad de los agentes que actúen de manera encubierta o con identidad falsa.*"

[487] No se comparte la decisión adoptada por el Juzgado Central de Instrucción nº 5 de la Audiencia Nacional en relación con una investigación por ciber-yihadismo. El titular de dicho juzgado autorizó, mediante la preceptiva resolución judicial, la utilización de dos agentes encubiertos online a fin de infiltrarse en un foro privado de internet que constituía un punto de encuentro de personas vinculadas con este tipo de terrorismo. Durante el desarrollo de la investigación, alguno o algunos de los miembros de dicho foro manifestaron a uno de los agentes que actuaban bajo identidad supuesta su voluntad de comunicarse con el vía telefónica. Ante este requerimiento, el agente encubierto online acudió al Juzgado solicitando una resolución judicial que le permitiera mantener este tipo de contactos a través del teléfono. Dicha resolución judicial fue finalmente concedida por el Juzgado Central de Instrucción nº 5 argumentando que en la medida que el agente online está habilitado, únicamente, para actuar en foros privados de comunicación en internet, para realizar este tipo de actuaciones de investigación en el mundo real (en el mundo físico) era necesario una resolución judicial adicional que le permitiera actuar como agente encubierto convencional en el mundo físico.
Esta nueva resolución es claramente redundante pues si dos agentes encubiertos online estaban legalmente autorizados para actuar como tales en canales cerrados de comunicación, y en el curso de dicha investigación se hizo necesario, además, el mantenimiento de contactos telefónicos con alguno de los investigados, la realización de estas comunicaciones no precisaba, a mi juicio, de una autorización judicial adicional pues no se producía, con estos actos, una vulneración del algún derecho fundamental que hiciera necesaria la misma. Se podía entender, en definitiva, que estos contactos telefónicos quedaban amparados bajo la primera resolución judicial.

El Juez podrá autorizar al agente encubierto informático a intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos (art. 282 bis 6 LECrim).

Se aborda un problema concreto que se estaba generando en determinadas investigaciones, normalmente relativas a foros de producción de pornografía infantil, en las que la prosecución de la investigación exige que el agente encubierto ponga a disposición de terceros archivos de contenido ilícito como forma de demostrar la personal sintonía con la actividad delictiva que se desarrolla en esos espacios virtuales. En estos casos la aportación de dicho material por parte del agente puede resultar condición ineludible para poder acceder a dichos foros y en consecuencia, para continuar la investigación.

La incorporación a la red de archivos de contenido ilícito puede poner en riesgo bienes jurídicos necesitados de protección, por lo que ha de ser autorizada de forma individualizada caso por caso, para que puedan valorarse criterios de necesidad de adecuación y de proporcionalidad. No pueden quedar al margen de esa valoración aspectos tales como el tipo de archivo ilícito que se pretende intercambiar o enviar; el destino de esos archivos y el control que pueda establecerse sobre el movimiento de los mismos en la red tanto en orden a la posibilidad de su posterior recuperación como para conjurar el riesgo de provocación delictiva.

No obstante, ha de advertirse que la dicción literal del precepto puede llevar también a la interpretación de que un archivo ilícito no es solamente aquel cuyo contenido puede vulnerar bienes jurídicamente protegidos, sino también el que contiene un software con un ejecutable cuyo cometido esté orientado a la investigación criminal. Un archivo ilícito puede tener muy distintas finalidades, algunas de las cuales pueden ser válidas para la investigación criminal, como monitorizar las pulsaciones del teclado, realizar capturas de pantallas o control y seguimiento de acciones del usuario, pero otras tienen una naturaleza claramente delictiva como la integración del dispositivo en una *botnet* (conjunto de robots informáticos que se ejecutan de manera autónoma y automática). Parece evidente que la introducción de un *software* no es la pretensión que subyace en la redacción del texto que se está examinando, pues esa posibilidad se encuentra regulada específicamente a propósito del registro remoto de equipos

informáticos, pero nada impide que el agente encubierto sea expresamente autorizado, de acuerdo con esa normativa, para utilizar esta técnica si ello fuera necesario[488].

Para evitar que el envío de archivos ilícitos se convierta en una provocación al delito han de quedar inequívocamente identificados[489]. En relación a la provocación delictiva existe una doctrina muy consolidada en la Sala Segunda del Tribunal Supremo a cuyo tenor: no cabe identificar ni confundir el delito provocado con el que ha venido a denominarse delito comprobado, que tiene lugar cuando la actividad policial, sin quebrar legalidad alguna, pretende descubrir delitos ya cometidos, generalmente de tracto sucesivo, toda vez que en estos supuestos el agente infiltrado no busca ni genera la comisión del delito, sino allegar pruebas de una ilícita actividad ya cometida o que se está produciendo, pero de la que únicamente se abrigan sospechas. En el delito provocado no se da en el acusado una decisión libre y soberana de delinquir. En el delito comprobado esa decisión es libre y nace espontáneamente[490].

---

[488] Informe del Consejo Fiscal al anteproyecto de LO de modificación de LECrim para la agilización de la justicia penal, el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Madrid 23 de enero de 2015. pág. 28.

[489] La identificación inequívoca de archivos informáticos se realiza ordinariamente a través del *hash* que es la clave alfanumérica resultante del análisis de los contenidos de cualquier archivo informático. Su especificidad es tal que la mas mínima alteración en el contenido del archivo determinaría la modificación de ese resultado *hash*. A su vez el termino algoritmo se emplea para definir los pasos e instrumentos necesarios para obtener un resultado como es precisamente el *hash*.

[490] SSTS 93/1999 de 16 de abril; 262/2003, de 19 de febrero y más reciente 427/2013, 10 de mayo. En última resolución además de dejar constancia de que el delito provocado es una rechazable e inadmisible actividad policial que traspasa los límites de la legalidad, recuerda expresamente que es clara la distinción entre el delito provocado instigado por la policía y aquella otra actividad policial tendente a acreditar el delito ya decidido de forma autónoma y libre por la persona concernida reduciéndose la actividad del agente policial a comprobar tal delito. En igual sentido ha de citarse la STEDH de 30 de octubre de 2014 (caso *Nosko y Nefedov* contra Rusia) que rechaza de plano la incitación policial como medio de investigación al quebrar la exigencia de un juicio justo.
También la Sentencia de Audiencia Nacional 13/2016, de 1 de junio, sostienen en relación a la figura del agente encubierto en un delito de tráfico de drogas que no existe delito provocado cuando los agentes de la autoridad sospechan o conocen la existencia de una actividad delictiva y se infiltran entre quienes la llevan a cabo, en busca de información o pruebas que permitan impedir o sancionar el delito. En estas ocasiones, la decisión de delinquir ya ha surgido firmemente en el sujeto con independencia del agente provocador, que, camuflado bajo una personalidad supuesta, se limita a comprobar la actuación del delincuente e incluso a realizar algunas actividades de colaboración con el mismo, en la actualidad reguladas en la LECrim. En estos caso, la actuación policial no supone una auténtica provocación, pues la decisión del sujeto activo siempre es libre y anterior a la intervención puntual del agente encubierto, aunque éste, siempre por iniciativa del autor de la infracción criminal, llegue a ejecutar labores de adquisición o transporte de los efectos del delito (art. 282 bis de la LECrim) u otras tareas de auxilio o colaboración similares, simulando así una disposición a delinquir que permite una más efectiva intervención policial. Jurisprudencia perfectamente aplicable al agente encubierto informático, siendo el envío de los archivos ilícitos perfectamente identificados, las tareas ejecutadas por el agente para simular su disposición a delinquir sin que pueda confundirse con la provocación delictiva.

Por último, los agentes encubiertos se encuentran habilitados, previa autorización judicial, para que en el curso de una investigación puedan grabar imágenes y conversaciones, incluido en el interior de un domicilio, cuando ello sea necesario. Se trata de la posibilidad de grabación de concretos encuentros, y no de una grabación de carácter continuado.

Ahora bien, dado el carácter reservado del agente encubierto en general e informático en particular, hay que garantizar adecuadamente su protección cuando la información por él suministrada acceda al plenario como material probatorio. De ahí la necesidad de garantizar desde el principio la reserva de su identidad.

En la práctica, resulta recomendable que la tramitación del procedimiento en el que se haya hecho uso del agente encubierto informático, se realice en dos piezas que se tramiten de forma separada de los autos principales[491]. La primera pieza se reserva a la identidad del agente encubierto informático, y por su especial sensibilidad se custodiará con las debidas garantías. Por ello, esta pieza nunca se unirá al procedimiento principal, cualquiera que sea la fase o estado procesal, aunque se hubiera alzado el secreto de las actuaciones. Podría ser objeto de remisión personal del Juzgado de Instrucción al Órgano judicial competente para el enjuiciamiento, debiendo en todo caso extremarse las precauciones dado su carácter reservado. Las partes no tendrán nunca acceso a su contenido, salvo el Ministerio Fiscal. Dicha pieza deberá contener:

- El código asignado al agente; así como los perfiles o redes sociales asignados a su actuación.

- La identidad real y supuesta del agente (con su número de identificación profesional) constará en un sobre cerrado o sistema similar, extremándose las medidas para garantizar su reserva de tal forma que nunca llegue a conocimiento de las partes (salvo el Ministerio Fiscal).

- Testimonio del oficio de la Unidad Policial actuante en el que se solicita la actuación del agente encubierto informático.

[491] Conclusiones de la II jornada sobre el marco jurídico de actuación del agente encubierto (Madrid, 29 de mayo de 2015). Ministerio de Justicia.

- Testimonio del informe favorable del Ministerio Fiscal.

- Auto original del Juez de Instrucción por el que se autoriza el agente encubierto informático.

- El código con el que a partir de ese momento se hará referencia al agente encubierto informático en actuaciones.

La segunda pieza separada se refiere al objeto de investigación del agente encubierto. También se tramitará en pieza separada y secreta. Una vez se alce la declaración de secreto de la pieza, las partes tendrán pleno acceso a su contenido, a excepción de aquellos pasajes de los que se infiera la identidad real o supuesta del agente encubierto a los que resulta de aplicación el carácter reservado previsto en la Ley.

La declaración de secreto de esta pieza separada puede alzarse en tiempo distinto de la declaración de secreto de los autos principales, pudiendo prolongarse más aquella. Y respecto a su contenido, incluirá:

- La solicitud de la unidad policial sobre la actuación del agente encubierto.

- El informe favorable del Ministerio Fiscal.

- Testimonio del auto habilitante de esa actuación, del que se excluirá la identidad real y ficticia, incluyéndose solamente el código.

- Informes de la actividad que el mismo vaya realizando y que presente a la autoridad judicial. Recogerá la información suministrada por el agente encubierto informático durante su investigación[492].

- Las eventuales actuaciones relativas a la voluntariedad de la actuación del agente[493], el tipo de archivo informático utilizado y su identificación con el código hash.

[492] En la forma y tiempo a los que se refiere la Conclusión 9 de la I Jornada. Conclusiones de la la II jornada sobre el marco jurídico de actuación del agente encubierto (Madrid, 29 de mayo de 2015). Ministerio de Justicia.

- Cualquier otra incidencia relacionada con su actuación; como puede ser, a título de ejemplo, la solicitud de autorización de medidas que supongan injerencia en un derecho fundamental.

Toda mención al agente encubierto se hará mediante el código asignado, tanto en oficios policiales como en resoluciones judiciales. Se sugiere la estandarización de este código vinculándolo a determinados conceptos: Identificación del Juzgado, año, número de procedimiento, número de agente, clase de perfil, número de perfiles asignados.

3.6 Hallazgo casual.

3.6.A) La doctrina del hallazgo casual en la jurisprudencia.

Obviamente, en la investigación de los ciberdelitos es necesario referirse a los hallazgos casuales descubiertos mediante diligencias de investigación tecnológicas, que son también de regulación *ex novo* tras la reforma de la LECrim en 2015.

Puede ser muy habitual que en el curso de cualquier investigación relacionada con el ciberdelito, que con el uso de estas técnicas, aparte de obtenerse información sobre las personas investigadas, aparezcan nombres o identidades de posibles proveedores o clientes, igualmente dedicados aparentemente a la misma actividad ilícita, o incluso, aparezcan otros delitos distintos, descubiertos por casualidad, diferentes de los inicialmente investigados. Dependiendo de lo descubierto, en ocasiones se permitirá la ampliación del procedimiento a unos y otros, o la deducción de testimonio de particulares para el inicio de una investigación criminal contra esas personas determinadas, al recabarse contra ellas indicios suficientes de criminalidad, o para la investigación de esos nuevos delitos.

[493]Teniendo en cuenta el contenido de la Conclusión 8 de la I Jornada. Conclusiones de la la II jornada sobre el marco jurídico de actuación del agente encubierto (Madrid, 29 de mayo de 2015). Ministerio de Justicia.

a) Hallazgo casual tras la práctica de un registro domiciliario.

Normalmente, la jurisprudencia del Tribunal Supremo se ha referido en reiteradas ocasiones a los supuestos de hallazgos casuales descubiertos tras la práctica de un registro[494], otorgando validez a la diligencia cuando, aunque el registro se dirigiera a la investigación de un delito específico, se encuentren efectos o instrumentos de otro que pudiera entenderse como delito flagrante. La teoría de la flagrancia ha sido, pues, una de las manejadas para dar cobertura a los hallazgos casuales, y también la de la regla de la conexidad de los arts. 17.5 y 300 LECrim, teniendo en cuenta que no hay novación del objeto de la investigación sino simplemente " *adición* ".

La Constitución no exige en modo alguno, que el funcionario que se encuentre investigando unos hechos de apariencia delictiva "cierre los ojos" ante los indicios de delito que se presentasen a su vista, aunque los hallados casualmente sean distintos a los hechos comprendidos en su investigación oficial, siempre que ésta no sea utilizada fraudulentamente para burlar las garantías de los derechos fundamentales (STC 49/1996, 26 de marzo).

El que se estén investigando unos hechos delictivos no impide la persecución de cualesquiera otros distintos que sean descubiertos por casualidad al investigar aquéllos, pues los funcionarios de policía tienen el deber de poner en conocimiento de la autoridad penal competente los delitos de que tuviera conocimiento, practicando incluso las diligencias de prevención que fueran necesarias por razón de urgencia, tal y como disponen los arts. 259 y 284 LECrim .

Pero esta doctrina de la validez del hallazgo casual presupone que el descubrimiento de los efectos que permiten afirmar la existencia de un segundo delito sumado al inicialmente perseguido, ha de producirse durante el desarrollo de una diligencia de registro no afectada de nulidad. Carecería de sentido que el hallazgo casual que aflora durante el desarrollo de un registro ilegal tuviera virtualidad para convertir

[494] Más reciente la STS 103/2015 de 24 de febrero que remite a la STS 48/2013, 23 de enero con cita de las SSTS 110/2010, 20 de febrero; 167/2010, 24 de febrero y 315/2003, 4 de marzo.

una vía de hecho inicialmente nula en un registro domiciliario constitucionalmente válido.

En resumen, para dar validez a los hallazgos casuales descubiertos tras la práctica de un registro, pudiendo hacerse extensivo al registro de dispositivos informáticos, se requiere según la jurisprudencia[495]:

a) Lo que realmente otorga validez a la práctica de un registro, cualquiera que fuere, no es sino la correcta habilitación judicial para la entrada en el domicilio.

b) Una vez cumplido tal requisito esencial, a partir de ese momento, la actuación policial discurre en un ámbito perfectamente legítimo, en sus dimensiones espacial y temporal, durante su transcurso íntegro.

c) Por ello, cualquier hallazgo que, en tales circunstancias, se produzca no puede ser tachado de irregular vista la legalidad en la que la diligencia discurre.

d) Si a ello se une, además, la concurrencia de la proporción entre la injerencia en el derecho fundamental y la gravedad del ilícito inesperadamente descubierto, la diligencia adquiere una imprescindible cobertura.

e) Tan sólo si se advirtiera que todo ello pueda responder, en realidad, a un designio intencionado de los funcionarios solicitantes del registro que fraudulentamente hubieren ocultado al Juez autorizante, por las razones que fueren, el verdadero motivo de su investigación, la violación del domicilio habría de ser considerada nula.

En definitiva, el hecho de hallar en un registro, válida y fundadamente autorizado en su origen, efectos u objetos distintos de los correspondientes al ilícito inicialmente investigado, no convierte en ilegal la práctica de la diligencia así realizada, de modo que si aquella inicial autorización reunió todos los requisitos exigibles para ser tenida como correcta, los hallazgos producidos como resultado de la misma, han de ostentar pleno valor probatorio.

[495] STS 17/2014 de 28 de enero [FJ 5º].

b) Hallazgo casual en escuchas telefónicas.

También existe reiterada jurisprudencia en relación a los hallazgos casuales descubiertos tras las escuchas telefónicas[496], que puede hacerse extensiva a las comunicaciones telemáticas y a los registros remotos, pues la autorización para las mismas no puede ser materialmente selectiva; es decir, ceñida a unas específicas conversaciones; no por mor de una regla jurídica o precepto normativo, sino por pura imposibilidad. No es factible, interceptado un teléfono, que se escuchen solo las conversaciones que puedan tener relevancia para la investigación y que el resto de comunicaciones no sean ni oídas, ni grabadas. A *priori* no puede discriminarse entre las conversaciones con interés criminal y aquéllas otras -que suelen ser la mayoría- irrelevantes a esos efectos. Solo tras escucharlas se podrán separar unas de otras.

Por tanto, la habilitación judicial para unas escuchas necesariamente ha de extenderse a todas las conversaciones que se efectúan por el número identificado y no solo las atinentes al delito objeto de investigación. No es irregular que se escuchen conversaciones no relacionadas con tal infracción. Si en el curso de esas escuchas surgen indicios de otro hecho criminal distinto del investigado (*hallazgo casual)* se impone la comunicación al juez instructor para ampliar, en su caso, el objeto de investigación.

De ello, es exponente la STS 616/2012, de 10 de julio en la que se declara, entre otros extremos, que "*aunque es cierto, que por la denominada doctrina del hallazgo casual se legitiman aquellas evidencias probatorias que inesperadamente aparecen en el curso de una intervención telefónica de forma totalmente imprevista, la doctrina de esta Sala Casacional, ha exigido que, para continuar con la investigación de esos elementos nuevos y sorpresivos, se han de ampliar las escuchas, con fundamento en el principio de especialidad, a través del dictado de una nueva resolución judicial que*

[496] STS 96/2015 de 5 de febrero. Ante la aparición de indicios de presunta dedicación al tráfico de drogas en el curso de las escuchas acordadas legítimamente en procedimiento seguido por otros posibles delitos, la policía lo comunicó al órgano judicial.

legitime tal aparición, y reconduzca la investigación, con los razonamientos que sean precisos, para continuar legalmente con la misma"[497].

c) Diferencias del hallazgo casual descubierto en un registro al descubierto en una intervención telefónica.

En materia de hallazgo casual la jurisprudencia destaca las diferencias existentes entre el descubierto durante la intervención telefónica y el descubierto en una entrada y registro[498], pudiendo hacerse extensiva a los descubiertos en la intervención de las comunicaciones telemáticas y registro remoto y a aquellos encontrados en el registro de dispositivos tanto por la distinta afectación de una y otra diligencia sobre la intimidad, verdaderamente más intensa y directa en la intervención telefónica, telemática y registro remoto como por la prolongación temporal de una y otra injerencia, pues la entrada y registro de dispositivos tiene acotada su duración temporal en una jornada y se desarrolla en unidad de acto, en tanto que la intervención de las comunicaciones y el registro remoto tienen una duración, respectivamente, de tres meses y un mes

[497] Es interesante, en este sentido, la STS 419/2013, de 14 de mayo, en la que en el curso de una investigación en la que se había autorizado la instalación de aparatos de escucha y grabación de las conversaciones en el interior de un vehículo policial al estar siendo investigado uno de los agentes como posible implicado en un delito de tráfico de drogas, se captó una conversación relativa a unos golpes dados a un detenido que iba en el vehículo. Se declaró la validez de la autorización judicial aunque se captase la conversación de otro agente que no estaba siendo investigado, pero que intervino en el delito de torturas descubierto accidentalmente. Y fundamentó la sentencia *que siempre que se acuerda una intervención telefónica se produce una recogida "de arrastre" de todas las conversaciones mantenidas a través del teléfono intervenido, sean de salida o de entrada, con la consecuencia de captar conversaciones ajenas al objeto de la investigación criminal que justificó la autorización judicial de la injerencia. De ahí no puede seguirse sin más la violación del derecho a la intimidad de las terceras personas cuyas conversaciones sean captadas. Lo procedente es efectuar una selección de lo relevante a la investigación y ocultar el resto, de suerte que no existe publicidad de esa parte privada.*
Hacía referencia a la Circular 1/2013 de la Fiscalía General del Estado, que sostenía que:*"....La propia naturaleza de la intervención determina que afecta no solo al titular de la línea sino también a sus interlocutores - SSTS 1001/2005* y *1717/1999 -. La intervención autorizada de las conversaciones alcanza no solo a aquel cuya línea telefónica es observada, sino también al interlocutor que se relaciona con el primero.... una intervención telefónica puede afectar los derechos de terceros ajenos a la investigación, sin que ello genere nulidades...."*.
En definitiva, que se grabase la conversación concernida al delito de torturas suponía un hallazgo casual derivado de una medida de injerencia válidamente adoptada y justificada aunque uno de los interlocutores de la conversación no fuera sospechoso del delito, inicialmente investigado. Por eso se trata, precisamente, de un hallazgo casual. No existió ninguna nulidad de tal conversación ni violación del derecho a la intimidad.

[498] STS 834/2015 de 23 de diciembre.

susceptible de ampliación y, consecuentemente, con unas facultades de control judicial distintos (cfr. STS 578/1995, de 28 de abril y STS 805/1997 de 7 de junio).

El motivo objeto de controversia era si el hallazgo novedoso a consecuencia de un registro, no relacionado con el delito investigado, podría ser introducido en un proceso distinto sin afectación del derecho a la inviolabilidad domiciliaria, o si, por el contrario, al no encontrarse entre el objeto autorizado del registro había de considerarse desprovisto de la cobertura judicial habilitante de la intromisión en el ámbito domiciliario y por tanto, obtenido como si tal resolución no le afectase.

En la jurisprudencia se han encontrado presentes ambos criterios. Así, en algunas sentencias se había reprochado a la comisión judicial que no hubiera suspendido la diligencia en el momento del hallazgo novedoso a fin de comunicar el mismo al Juez autorizante y reclamar de éste una resolución distinta que amparase la investigación del nuevo delito. Así las SSTS 343/1994 de 18 de febrero y 1225/1995 de 1 de diciembre, señalan que si el registro va más allá del mandato judicial e investiga otros delitos conexos o no, será nulo en lo relativo a los excesos, si el juez instructor no amplía su mandato respecto al objeto del registro.

Esta línea jurisprudencial trasladaba al ámbito del registro domiciliario la tesis elaborada con ocasión de los descubrimientos casuales ocurridos en el curso de una intervención telefónica, en la que el principio de especialidad adquiere especial relevancia y justifica la intervención solo al delito investigado, en evitación de "rastreos" indiscriminados de carácter meramente preventivos o aleatorio sin base fáctica previa de la comisión de delito, absolutamente proscritos en nuestro ordenamiento.

No obstante, la jurisprudencia más reciente[499], ha abandonado dicha interpretación y establece que si en la práctica del registro aparecen objetos constitutivos de un cuerpo de posible delito distinto a aquel para cuya investigación se extendió el mandamiento habilitante, tal descubrimiento se instala en la nota de

[499] Por todas, la STS 834/2015, de 23 de diciembre a la que se ha hecho referencia, la STS 558/2014 de 8 de julio y STS 419/2013 de 14 de mayo. También las SSTS 539/2011, de 26 de mayo y 1110/2010, de 23 de diciembre.

flagrancia por lo que producida tal situación la inmediata recogida de las mismas no es sino consecuencia de la norma general contenida en el art. 286 de la Ley Procesal.[500]

El hecho de que la autorización judicial para la entrada y registro se ciña a actividades delictivas concretas, no supone que el hallazgo de efectos o instrumentos que se refieren a conductas delictivas distintas queden desamparados de la autorización judicial que cubre la intromisión en la esfera privada que entraña un registro[501]. No se puede seguir, el mismo criterio que cuando se trata de un intervención telefónica. Ésta, por su propia naturaleza, presupone una prolongación temporal que permite, en los casos de escuchas referidas a otras conductas delictivas distintas, una ampliación de la autorización judicial habilitante. Mientras que el registro se caracteriza por su realización en unidad de acto. Por ello, es preciso que el registro esté debidamente autorizado, aun cuando lo fuera con la finalidad de descubrir un delito distinto, y que el hallazgo se produzca de buena fe[502].

---

[500] En igual sentido, la STS 167/2010, de 24 de febrero, recoge la doctrina de otras sentencias precedentes como la 315/2003, de 4 de marzo, que admitió la validez de la diligencia cuando, aunque el registro se dirigiera a la investigación de un delito, se encontraran efectos o instrumentos de otro que pudiera entenderse como delito flagrante. La teoría de la flagrancia ha sido, pues, una de las manejadas para dar cobertura a los hallazgos casuales, y también la de la regla de la conexidad de los arts. 17.5 y 300 LECrim, teniendo en cuenta que no hay novación del objeto de la investigación sino simplemente "adición".
En igual sentido, la STS 1149/1997 de 26 de septiembre que, referida a un encuentro casual de efectos constitutivos de un delito distinto del que fue objeto de la injerencia, admite su validez siempre que se observen los requisitos de proporcionalidad y que la autorización y práctica se ajusten a los requisitos y exigencias legales y constitucionales. *"Si las pruebas casualmente halladas hubieran podido ser obtenidas mediante el procedimiento en el que se encontró, nada impide que tales pruebas puedan ser valoradas";* y la STS 465/1998, de 30 de marzo, "se ha impuesto en la doctrina de esta Sala una posición favorable a la licitud de la investigación de aquellas otras conductas delictivas que nacen de los hallazgos acaecidos en un registro judicialmente autorizado". En la jurisprudencia del Tribunal Constitucional se recoge un idéntico criterio y en la STC 41/1998, de 24 de febrero, afirma que "*...el que se estén investigando unos hechos delictivos no impide la persecución de cualesquiera otros distintos que sean descubiertos por casualidad al investigar aquéllos, pues los funcionarios de Policía tienen el deber de poner en conocimiento de la autoridad penal competente los delitos de que tuviera conocimiento, practicando incluso las diligencias de prevención".*

[501] Con similar criterio se pronuncia la STS 768/2007, de 1 de octubre, en la que se declara que la doctrina de esta Sala ha entendido que el hecho de que el hallazgo de elementos probatorios de un determinado delito se produzca en el curso de la investigación autorizada para otro delito distinto no supone la nulidad de tal hallazgo como prueba de cargo. En la STS 885/2004, de 5 de julio, se decía que "*Las Sentencias de esta Sala, 1004/1999, de 18 de junio , y 1990/2002, de 29 de noviembre, sientan la doctrina de que si el hallazgo es casual, no por ello deja de tener valor lo encontrado, siempre que estemos en presencia de flagrancia delictiva...". Para ello es preciso que el registro esté debidamente autorizado, aun cuando lo fuera con la finalidad de descubrir un delito distinto, y que el hallazgo se produzca de buena fe* (STS 1093/2003, de 24 de julio y STS 742/2003 de 22 de mayo).

[502] SSTS 1110/2010, 23 de diciembre y 981/2003, 3 de julio que afirman: "*...el hallazgo de elementos o datos directos o indiciarios de la comisión de un delito distinto del que dio lugar a la iniciación de las*

Además, no existe obstáculo a recibir el hallazgo casual tras la información de investigaciones llevadas a cabo por servicios policiales extranjeros (STS 862/2012, de 31 de octubre)[503].

3.6.B) La regulación del hallazgo casual en la LECrim.

La LECrim, de conformidad con la jurisprudencia examinada, regula los hallazgos casuales con motivo de la adopción de medidas de investigación tecnológica, en el artículo 588 bis i, que efectúa a su vez una remisión espresa al artículo 579 bis LECrim.

Lo primero que llama la atención es que el hallazgo casual puede producirse en todas y cada una de las diligencias de investigación reguladas en el capítulo IV del Título VIII del Libro II. A diferencia, por ejemplo, del borrador de código procesal penal que tan solo contemplaba los hallazgos casuales en relación al registro domiciliario (art. 344), pero no para el registro de dispositivos o registro remoto.

Se ha resaltado en este capítulo que para adoptar alguna de estas medidas de investigación tecnológica se requiere autorización judicial motivada para descubrir un delito concreto conforme al principio de especialidad. No es admisible acordar una diligencia de investigación tecnológica para tratar de descubrir, en general, sin la adecuada precisión, actos delictivos, ni extender una autorización prácticamente en blanco, siendo exigible concretar el fin del objeto de la investigación y que éste no sea rebasado[504].

---

investigaciones, la doctrina más reciente de esta Sala viene estableciendo, en lo que respecta a los descubrimientos casuales de pruebas de otro delito distinto del inicialmente investigado, la posibilidad de su validez y de la adjudicación de valor probatorio a los elementos encontrados, siempre que se cumpla con el principio de proporcionalidad y que la autorización y la práctica del registro se ajuste a las exigencias y previsiones legales y constitucionales".

[503] STS 157/2014, de 5 de marzo.

[504] *Vid*. STS 818/2011, de 21 de julio y STS 372/2010, de 29 de abril.

Dicho esto, ha de tenerse presente lo ya señalado acerca de que la Constitución no exige, en modo alguno, que el funcionario que se encuentra investigando unos hechos de apariencia delictiva "cierre los ojos" ante los indicios de delito que se presentaren a su vista, aunque los hallados casualmente sean distintos a los hechos comprendidos en su investigación oficial, siempre que ésta no sea utilizada fraudulentamente para burlar las garantías de los derechos fundamentales[505]. En estos casos no puede renunciarse a investigar la *notitia criminis* incidentalmente descubierta en una intervención dirigida a otro fin, aunque ello precisa una nueva autorización judicial específica de la que aquélla sea mero punto de arranque[506].

El tratamiento de los denominados descubrimientos casuales tiene mucho que ver con el principio de especialidad aludido, y supone la aparición en el ejecución de una determinada intervención de indicios acerca de la comisión de otras infracciones no contempladas en la resolución habilitadora inicial, cuya persecución deberá ser autorizada expresamente por el juez, postura jurisprudencial que se traslada a la ley sin reservas (art. 579 bis.3 por remisión del art. 588 bis i).

De ahí que la continuidad en la investigación de un hecho delictivo nuevo requiera de una renovada autorización judicial (STS 740/2012, de 10 de octubre)[507].

---

[505] Circular 1/2013 de la Fiscalía General del Estado, sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas (SSTC 41/1998, de 24 de febrero y 49/1996, de 26 de marzo).

[506] El trascendente ATS de 18 de junio de 1992 (rec. 610/1990) abrió camino al señalar que "*respecto al problema de la divergencia entre el delito objeto de investigación y el que de hecho se investiga…basta con que, en el supuesto de comprobar la policía que el delito presuntamente cometido, objeto de investigación a través de interceptaciones telefónicas, no es el que se ofrece en las conversaciones que se graban, sino otro distinto, para que dé inmediatamente cuenta al Juez a fin de que éste, conociendo las circunstancias concurrentes, resuelva lo procedente"*.
De no obrar de este modo, en otro caso, la autorización, de hecho, se transforma en una especie de persecución del comportamiento genérico de una o varias personas a través de las conversaciones telefónicas, lo cual es totalmente inaceptable.

[507] En este sentido, es paradigmático el ATC 400/2004, de 27 de octubre que declara que *"pueden ser utilizados los hallazgos casuales producto de escuchas para deducir actuaciones contra los que resultaren implicados en delito grave por las mismas…la utilización en este caso del hallazgo casual ha resultado plenamente respetuosa con las exigencias que pudieran derivarse del reconocimiento constitucional del derecho al secreto de las comunicaciones, puesto que aquél ha sido utilizado como mera notitia criminis que se ha hecho llegar inmediatamente al órgano judicial competente, sin que se haya procedido a continuar con unas escuchas que ya entonces no hubiesen tenido cobertura en el auto de intervención citado*". Si los hechos descubiertos no guardasen conexión con los causantes del acuerdo de la medida y aparentan una gravedad penal suficiente como para tolerar proporcionalmente su adopción, se estimarán como mera "notitia criminis" y se deducirá testimonio para que, siguiendo las normas de competencia territorial y en su caso las de reparto, se inicie el correspondiente proceso (STS

Para la utilización del resultado de estas diligencias en otro proceso penal distinto, se requiere un nuevo auto judicial que lo convalide. Para ello, es exigible que en la deducción de testimonio de particulares se incluya lo necesario para acreditar la legitimidad de la injerencia en la que se haya producido el hallazgo casual. Una de las cuestiones que habrá que analizar es precisamente el marco en el que se ha producido el hallazgo casual y que no esté viciado de nulidad. Esto es, si las diligencias de investigación tecnológica traen causa o derivan de las practicadas en otro procedimiento distinto, se plantea la necesidad de analizar la validez de las practicadas en el primer procedimiento para decidir sobre la validez de las practicadas en el segundo, ya que la nulidad de las primeras determinaría irremediablemente la nulidad de las segundas por el efecto reflejo que dimana del artículo 11 de la LOPJ.

La cuestión relativa a la impugnación del hallazgo casual por la falta de la legitimidad de las diligencias de investigación adoptadas en un proceso penal precedente, fue abordada por el Pleno no jurisdiccional de la Sala Segunda del Tribunal Supremo de 26 de mayo de 2009, que alcanzó el siguiente Acuerdo[508]: "*En los procesos incoados a raíz de la deducción de testimonios de una causa principal, la simple alegación de que el acto jurisdiccional limitativo del derecho al secreto de las comunicaciones es nulo, porque no hay constancia legítima de las resoluciones antecedentes, no debe implicar sin más la nulidad. En tales casos, cuando la validez de un medio probatorio dependa de la legitimidad de la obtención de fuentes de prueba en otro procedimiento, si el interesado impugna en la instancia la legitimidad de aquel medio de prueba, la parte que lo propuso deberá justificar de forma contradictoria la legitimidad cuestionada. Pero, si, conocido el origen de un medio de prueba propuesto en un procedimiento, no se promueve dicho debate, no podrá suscitarse en ulteriores instancias la cuestión de la falta de constancia en ese procedimiento de las circunstancias concurrentes en otro relativas al modo de obtención de las fuentes de aquella prueba.*"

940/2011, de 27 de septiembre). No obstante, la resolución judicial que legalice la investigación de los hallazgos casuales o fortuitos la puede dictar el juez instructor del delito originario, si el delito es conexo.

[508] Se adoptó un Acuerdo que, en buena medida, toma como inspiración la doctrina sentada en la STS 503/2008, 17 de julio.

La lectura íntegra del Acuerdo de 26 de mayo de 2009 conlleva, según explica la STS 503/2012, de19 de junio, lo siguiente[509]:

a) que no existen nulidades presuntas;

b) que la prueba de la legitimidad de los medios de prueba con los que pretenda avalarse la pretensión de condena, incumbe a la parte acusadora;

c) pese a ello, la ley no ampara el silencio estratégico de la parte imputada, de suerte que si en la instancia no se promueve el debate sobre la legalidad de una determinada prueba, esa impugnación no podrá hacerse valer en ulteriores instancias.

Este acuerdo jurisdiccional ha sido después aplicado en diferentes Sentencias, algunas de las cuales declararon la nulidad de las intervenciones telefónicas por no haberse aportado a la nueva causa las resoluciones del procedimiento de donde procedían las escuchas que generaron las fuentes de prueba que acabaron operando en el nuevo proceso[510].

---

[509] En la STS 272/2011 de 12 de abril, se recuerda que: "*Nos encontramos, por tanto, con un procedimiento diferente en el que todas las escuchas se han realizado mediante las oportunas resoluciones judiciales, constando que la primera noticia surge con ocasión de otra investigación, en la que las escuchas estaban amparadas por una resolución judicial y, como recuerda la STS 187/2009, no es procedente presumir que las actuaciones judiciales y policiales son ilegítimas e irregulares y por ende vulneradoras de derechos fundamentales, mientras no conste lo contrario. "El presupuesto del razonamiento debe ser el opuesto al recurrente y, por tanto, debe partirse de que salvo prueba en contrario hay que suponer que los jueces, policías, autoridades y en general funcionarios públicos han adecuado su actuación a lo dispuesto en las leyes y en la Constitución. sería absurdo presumir que como no constan las actuaciones iniciales obrantes en una causa distinta hay que entender que no hubo autorización judicial de la intervención o la misma fue inmotivada o injustificada. Como bien apunta el Fiscal, ni el derecho a la presunción de inocencia ni el principio procesal "in dubio pro reo" llega hasta el punto de tener que presumir por mandato constitucional que, salvo que se acredite lo contrario, las actuaciones de las autoridades son ilegítimas e ilícitas".*

[510] STS 1130/2009, de 10 de noviembre se refiere a un supuesto en que el origen de la investigación judicial que concluyó con la resolución recurrida se encontraba en otras diligencias previas de las que se desgajaron las que dieron lugar a la nueva causa, y sin embargo no se figuraban en ella ni la petición inicial de la policía de la intervención telefónica ni el subsiguiente auto autorizante, por lo que se desconocía si la injerencia inicial, con sacrificio del derecho a la privacidad de las comunicaciones, estuvo justificada en virtud de los datos que pudiera haber facilitado la policía. De modo que -dice la referida sentencia- *al efectuarse el desglose se omitieron los antecedentes necesarios de donde derivaban las investigaciones desglosadas, es decir, no se adjuntó testimonio del oficio policial inicial de solicitud de autorización ni de las resoluciones judiciales autorizantes hasta enlazar con las diligencias desglosadas por lo que se acuerda la nulidad de toda la intervención telefónica y la de todas las pruebas derivadas de la misma (art. 11.1 LOPJ). Esta Sala, una vez acreditado que la cuestión se había suscitado ya en la instancia y que sin embargo no se habían aportado los antecedentes de la intervención telefónica, resalta en la citada sentencia 1130/2009 la extraordinaria importancia del primer auto judicial autorizante de la intervención telefónica, porque en él se acordó la injerencia inicial, y por tanto debe estar basado en datos concretos y objetivos acerca de la existencia de la comisión del delito para el*

Para evitar estos problemas el art. 579.2 LECrim exige la deducción de testimonio del procedimiento en el que se obtuvo el dato y su incorporación al nuevo procedimiento en el que se investiga la actividad delictiva descubierta. Por ello, habrá de analizarse y así debe incluirse entre los antecedentes indispensables, la solicitud inicial para la adopción, la resolución judicial que la acuerda y todas las peticiones y resoluciones judiciales de prórroga recaídas en el procedimiento de origen.

Se deja, sin embargo, sin solventar la duda sobre si la iniciativa para la deducción de testimonio debe proceder siempre del Juez que haya ordenado la intervención; o cabe la posibilidad de que un Juez distinto, por razón de una competencia objetiva o territorial, tras petición específica de la Policía Judicial que se hubiera encargado de llevar a efecto el acto de injerencia o tenido un conocimiento legítimo de tal investigación, recabe tales testimonios del Juez que hubiera acordado la injerencia o de quien finalmente hubiera conocido de su enjuiciamiento. Cualquiera de las dos opciones podría ser legítima; pues permitirá siempre la realización por una autoridad judicial de un ponderado análisis sobre si concurren o no las circunstancias objetivas exigidas en el ap. 1.[511]

La regulación legal añade un plus al control judicial de estas hipótesis cuyo objetivo no es otro que evitar investigaciones prospectivas, para lo cual se exige que el juez verifique "*la diligencia de la actuación, evaluando el marco en que se produjo el hallazgo casual y la imposibilidad de haber solicitado la medida que lo incluyera en su momento*" (art. 579 bis 3 LECrim). Ello no significa que deba exigirse a los agentes actuantes una diligencia especial, pero sí la ordinaria en el desempeño de sus tareas

---

que se solicita la intervención y de la posible intervención en él del usuario del teléfono cuya intervención se solicita. Pues es en este primer auto donde en toda su amplitud debe efectuarse por el juez el juicio de ponderación que justifique el sacrificio del derecho fundamental protegido en el art. 18.3º de la Constitución, y por tanto donde debe verificarse la proporcionalidad, idoneidad y excepcionalidad de la medida. Y como resulta imprescindible la exigencia de un efectivo control judicial, absolutamente necesario como valladar a los riesgos que pueden conllevar esa vía excepcional de investigación que lleva ínsito el riesgo de expansión que tiene, paradójicamente, toda medida excepcional (SSTS 998/2002; 498/2003;182/2004 y 280/2004), acaba considerando, ante la falta de control judicial de la intervención telefónica inicial, como consecuencia prevista en el Acuerdo de 26 de mayo de 2009, la nulidad de toda la intervención telefónica y la de todas las pruebas derivadas de la misma (art. 11.1 LOPJ). En la misma dirección se pronunciaron las SSTS 605/2010, de 24 de junio, 744/2010, de 26 de julio, 1138/2010, de 16 de diciembre.

[511] RODRÍGUEZ LAINZ, J. L. "La interceptación de las comunicaciones telefónicas y telemáticas en el Anteproyecto (…)". ob. cit. pág. 15.

investigadoras como garantía frente a una utilización fraudulenta de los recursos que les proporciona la ley[512].

No obstante, no se vulnera la especialidad y ésta se da cuando no se produce una novación del tipo penal investigado, sino una adición o suma (STS 792/1997, de 30 de mayo).

Tampoco la aparición de cualquier indicio de la comisión de un delito distinto del investigado impone una inmediata dación de cuenta al Juez para que éste, sin solución de continuidad, dicte una nueva resolución. Debe tenerse presente que el objeto del proceso es de cristalización progresiva. No responde a una imagen estática, en la que toda irrupción de un indicio deba conllevar una resolución jurisdiccional que renueve la delimitación objetiva y subjetiva originariamente definida. Esa delimitación, desde luego, es obligada, pero no a raíz del primer indicio, sino cuando la suma de todas ellos y otros datos indiciarios, permitan al Juez instructor, detectar los elementos que justificarían una renovada motivación y una investigación desgajada de la causa matriz. Desde que se dibujan los primeros y tenues trazos incriminatorios, hasta que los indicios adquieren el significado preciso para justificar un nuevo auto de injerencia, es lógico que pase el tiempo indispensable para que los agentes de policía que llevan a cabo el seguimiento puedan detectar la información, analizarla, interrelacionarla y, por último, dar cuenta a la autoridad judicial[513]. Lo decisivo es, al fin y al cabo, que el Juez instructor, desde el primer momento, tenga conocimiento del desarrollo de las investigaciones, que sepa el resultado que van arrojando, sin que se avalen espacios de injerencia ajenos a la garantía constitucional que reconoce el art. 18. de la CE[514].

[512] CABEZUDO RODRÍGUEZ, N. "Ciberdelincuencia e investigación criminal (…) ob. cit. pág. 35.

[513] Circular 1/2013 de la Fiscalía General del Estado sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas.

[514] STS 636/2012, de 13 de julio "*Lo que se pide del órgano jurisdiccional en supuestos…en los que el núcleo inicial de las investigaciones se enriquece con otros hallazgos imprevistos, también de significado jurídicopenal, es que dicte una resolución que justifique el sacrificio del derecho a la inviolabilidad de las comunicaciones para la investigación del nuevo delito y la determinación de sus hipotéticos responsables. Y que lo haga sin demoras injustificadas, actuando desde que cuente con los indicios imprescindibles para razonar la conveniencia de un sacrificio añadido en los derechos fundamentales la cristalización del objeto del proceso se verifica de forma paulatina y, por tanto, ajena a respuestas súbitas".*

Por último, tras dar traslado del descubrimiento casual al Juez instructor, habrá de informarse si las diligencias de investigación tecnológica continúan declaradas secretas, a los efectos de que tal declaración sea respetada en el otro proceso penal, y se comunicará el momento en el que dicho secreto se alce.

CAPÍTULO OCTAVO.

LA PRUEBA DE LOS CIBERDELITOS.

1. NATURALEZA JURÍDICA DE LA PRUEBA DE LOS CIBERDELITOS.

Las peculiaridades en torno a la prueba de los ciberdelitos vienen suscitadas por el hecho de la singularidad propia de estos delitos, en los que para la averiguación del hecho típico y de las personas responsables hay que tener en cuenta que la comisión de los mismos tiene lugar en un ámbito inmaterial -el espacio virtual o cibernético-, constituido por las redes telemáticas, en el que la información y acreditación del hecho no sólo viene representado por datos electromagnéticos, eminentemente volátiles, sino que tanto su comisión así como su constatación por el ser humano precisa de unos elementos físicos, constituidos por los equipos informáticos y telemáticos[515].

Una primera cuestión que se encuentra a la hora de estudiar la prueba de los ciberdelitos es la diversa denominación que recibe. Así, se habla de prueba electrónica, telemática, informática o digital, indistintamente. Parece que el término más correcto desde un punto de vista técnico es el de prueba informática[516], pues una de las bases de la informática es la electrónica, pero no la única, ya que para que se pueda tratar de forma automática la información por medio de ordenadores, además del movimiento de

[515] ROVIRA DEL CANTO, E "Las nuevas pruebas telemáticas (…)". ob. cit. pág. 285.

[516] Según el DRAE, **"Electrónica"** es el "*estudio y aplicación del comportamiento de los electrones en diversos medios, como el vacío, los gases y los semiconductores, sometidos a la acción de campos eléctricos y magnéticos"*. "**La Informática"**, es el *"conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores*. **"La telemática"** *es "la aplicación de las técnicas de la telecomunicación y de la informática a la transmisión de información computarizada*". "**Digital",** "dicho de un aparato o de un sistema: *Que presenta información, especialmente una medida, mediante el uso de señales discretas en forma de números o letras"*. Diccionario de la Lengua Española, R.A.E., vigésima segunda edición, 2001, tomos I y II.

los electrones y, por tanto, de la electrónica, es necesaria la intervención de otras disciplinas[517].

Teniendo en cuenta que existen tecnologías emergentes que no se basan en la electrónica, al menos en cuanto al cómputo o almacenamiento de la información y que términos como "electrónica" o "digital" no coinciden con la disciplina que trata esos elementos (que es la informática) quizás sería conveniente unificar y simplificar vocabulario alrededor de este último termino: informática[518]. Hablar de prueba electrónica carece de sentido desde el momento en que no se puede obtener ninguna información útil para el proceso judicial con un acceso directo a los electrones que componen las evidencias informáticas, no siendo siquiera posible realizar dicho acceso. Lo mismo es predicable respecto al término dispositivo electrónico, siendo el técnicamente correcto el de informático pues, la informática se sitúa, en un orden de abstracción superior a la electrónica[519].

En la práctica, se viene entendiendo que constituye *prueba informática* toda la información generada, almacenada o transmitida mediante el uso de dispositivos informáticos que tiene aptitud para acreditar el hecho objeto de enjuiciamiento. Así se define[520] a la prueba informática como toda información de valor probatorio contenida en un medio informático o transmitida por dicho medio.

---

[517] RUBIO ALAMILLO, J. "La informática en la reforma de la Ley de Enjuiciamiento Criminal". Diario La Ley nº 8662, Sección Tribuna, 10 de diciembre de 2015. pág. 2. "*Un aparato electrónico propiamente dicho es un televisor, una nevera o una lavadora y, es evidente que este tipo de electrodomésticos no pueden ser utilizados para cometer delitos informáticos, pues no se pueden ejecutar programas sobre ellos (aunque la tecnología domótica está avanzando mucho y ya existen electrodomésticos capaces de conectarse a Internet y realizar ciertas funciones básicas, como ordenar la compra, pero el usuario tiene una interacción extraordinariamente limitada o incluso nula con dichos programas). Sin embargo, en ningún momento se puede considerar a un ordenador como un aparato puramente electrónico, ya que los programas que se ejecutan sobre el mismo realizan funciones muy complejas que necesitan obligatoriamente de la interacción del usuario y, por tanto, el ordenador sí puede ser utilizado para cometer actividades delictivas. Un ordenador, por tanto, debería considerarse como una prueba informática y no electrónica.*"

[518] ANGUAS BALSERA, J. La cadena de valor en la prueba con base informática. http://www.anguas.com/e1m6/Docs/Foro_Legal_La%20cadena_de_valor_de_la_prueba_informatica.pdf

[519] RUBIO ALAMILLO, J. "La informática en la reforma de la Ley de Enjuiciamiento Criminal". ob. cit. pág. 2. Siguiendo la misma lógica, un disco duro y una memoria de almacenamiento masivo también son dispositivos informáticos, ya que la información ha sido almacenada en los mismos a través de sistemas informáticos (ordenadores y redes de ídem) y no electrónicos (electrodomésticos y asimilados).

[520] DELGADO MARTIN, J. "La prueba electrónica en el proceso penal". Diario La Ley nº 8167, Sección Doctrina, 10 Octubre 2013. pág. 1 define así a la prueba electrónica.

En esta definición se destacan los siguientes elementos: se refiere a información que ha ser producida, almacenada o transmitida por medios informáticos y que pueda tener efectos para acreditar hechos en el proceso abierto para la investigación de todo tipo de infracciones penales, y no solamente para los denominados ciberdelitos[521].

De esta manera, la fuente de la prueba radica en la información contenida o transmitida por medios informáticos, mientras que el medio de prueba será la forma a través de la cual esa información entra en el proceso: normalmente como prueba documental o como prueba pericial, pero también incluso a través de la prueba testifical mediante el testimonio de la persona que ha tenido contacto con el dispositivo informático.

Entre la acreditación del hecho ilícito y la averiguación del presunto responsable penal, siguiendo los criterios procesales clásicos y tradicionales, debe procederse a la investigación y acreditación de los elementos físicos con los que se opera en la red: el equipo origen de la acción delictiva, los servidores y nodos por los que la información ilícita o los datos o archivos que va a materializar el ilícito transitan, los equipos y terminales de paso inoperante o inactivo, y los sistemas, terminales o equipos finales a donde la información es transmitida, recibida, opera, se transforma o afecta. Y todo ello debe ser objeto formal de prueba[522], para lo que es necesario que se adopten precauciones y medidas especiales para que puedan servir de prueba ante los tribunales.

Es, por tanto, un medio de prueba nacido por el avance de la tecnología en el ámbito de la información y comunicación, reconocido como medio de prueba autónomo en el art. 299.2 de la Ley de Enjuiciamiento Civil (LEC)[523], según el cual también se admitirán como medios de prueba a usar en juicio "*los medios de reproducción de la*

---

[521] *Vid.* GÓMEZ ORBANEJA, E Y HERCE QUEMADA, V. "Derecho Procesal Penal". Madrid, 1972. Distingue a la prueba como actividad, como fuente y como medio.

[522] ROVIRA DEL CANTO, E. "Las nuevas pruebas telemáticas (…)". ob. cit. pág. 286.

[523] *Vid.* NIEVA FENOLL, J. La prueba en documento multimedia, en "Instituciones del nuevo proceso civil" (AA.VV), Vol. II. Economist&Iurist, Barcelona, 2000. pág. 451.
El artículo 299 de la LEC que relaciona los medios de prueba que pueden emplearse en juicio instaurando un sistema de números *apertus* donde se permite la utilización de "cualquier otro medio de prueba no expresamente previsto", si del mismo "pudiera obtenerse certeza sobre hechos relevantes". Aplicable al proceso penal de forma supletoria conforme a su art. 4.

palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso".

Asimismo, el artículo 384.1 de la misma ley permite su introducción en el proceso al sostener que tales instrumentos "*serán examinados por el tribunal por los medios que la parte proponente aporte o que el tribunal disponga utilizar y de modo que las demás partes del proceso puedan, con idéntico conocimiento que el tribunal, alegar y proponer lo que a su derecho convenga"*, pudiéndose complementar con los dictámenes y medios de prueba instrumentales que la parte considere convenientes y aporte, conforme a lo dispuesto en el art. 382.2 LEC, así como las otras partes.

En ambos casos, tanto en relación con las reproducciones como con los instrumentos en sí, el tribunal efectuará su valoración *conforme a las reglas de sana crítica aplicables a aquellos según su naturaleza* (arts. 382.3 y 384.3 LEC).

También el artículo 230 LOPJ autoriza a los Juzgados y Tribunales a utilizar cualquier otro medio técnico, electrónico, informático y telemático para el desarrollo de la actividad y el ejercicio de sus funciones. Añadiendo que los documentos emitidos por los medios anteriores, cualquiera que sea su soporte, gozarán de la validez y eficacia de un documento original siempre que quede garantizada su autenticidad, integridad y el cumplimiento de los requisitos exigidos en las leyes procesales[524].

En lo que concierne a la admisibilidad de las pruebas informáticas en el proceso penal, se aplican en esta materia las normas generales sobre admisibilidad de la prueba de la LECrim.

Se ha visto en el capítulo anterior cómo la Ley de Enjuiciamiento Criminal regula expresamente la forma y garantías que han de observarse para la práctica de las diligencias de investigación tecnológica en diversos apartados de su articulado, con el

[524] SANCHÍS CRESPO, C. *La prueba en soporte electrónico*, en "Las Tecnologías de la Información y de la Comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio" (Gamero Casado y Valero Torrijos, coord.). Ed. Thomson Reuters Aranzadi, Navarra, 2012, pág. 708. "*Posteriormente la Ley 59/2003, de 19 de diciembre, de Firma electrónica, confirmó la tendencia de equiparación ya existente, entre los documentos tradicionales, en soporte papel o similar, y los electrónicos. Su artículo 3.8 disponía que el soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio*".

fin de que su correcta obtención y tratamiento aseguren su valor como fuente de prueba al reunir los necesarios requisitos de validez sustancial, formal y procesal.

Esta regulación legal ha solventado buena parte de los problemas de legalidad a los que había que enfrentarse a la hora de adoptar alguna de las medidas de investigación tecnológica, principalmente porque viene a dar cobertura legal a estas técnicas. No obstante, debería ser completada con una normativa reglamentaria que regulase aspectos y singularidades con la finalidad de garantizar su autenticidad e integridad, o las diferentes cuestiones sobre la realización de la prueba pericial informática, entre otras[525], de modo que permita que la actuación del sistema penal pueda ir adaptándose a las nuevas realidades, compatibilizando la flexibilidad con las necesidades de la seguridad jurídica, teniendo en cuenta las recomendaciones y otros documentos elaborados por entidades con reconocimiento científico (como por ejemplo la *ENFSI-European Network of Forensic Science Institutes*)[526].

En cuanto a su naturaleza, la prueba informática se plantea e introduce en el proceso considerando que tiene naturaleza de prueba documental. Esta es la opinión mayoritaria de la doctrina y jurisprudencia[527], por las semejanzas que guarda el soporte electrónico con el documento y por la idoneidad de su introducción al proceso como tal. Se apoya este criterio en lo dispuesto en el artículo 26 del Código Penal, conforme al

[525]DELGADO MARTIN, J. "La prueba electrónica en el proceso penal". ob. cit. pág. 2. "*Esta necesidad deviene aún más relevante si se tienen en cuenta los rápidos avances en las tecnologías de la información y de la comunicación, que generan nuevas necesidades (realidad criminológica) y elementos (modernas técnicas para acreditar los elementos de la infracción penal) en la investigación de los delitos".*

[526] European Network of Forensic Science Institutes: http://www.enfsi.org
Miembros de España: Criminalistic Service of the Civil Guard, Madrid; Forensic Science Unit. Basque Country Police. Spain. (FSU), Erandio; General Commissary of Scientific Police (GCSP), Madrid; National Institute of Toxicology and Forensic Science, Madrid; Scientific Police Division (CME), Sabadell.

[527] Así ya desde la Sentencia del Tribunal Supremo de 3 de noviembre de 1997, Sala 3ª, (rec. 544/1995) [FJ 10º]. "*La virtualidad jurídica del documento en soporte electrónico versa, principalmente, sobre la problemática de su admisión -siempre que se den todas las cautelas necesarias para cerciorarse de su autenticidad- como prueba procesal(...) Estamos asistiendo, en cierto modo, en algunas facetas de la vida, incluso jurídica, al ocaso de la civilización del papel, de la firma manuscrita y del monopolio de la escritura sobre la realidad documental. El documento, como objeto corporal que refleja una realidad fáctica con trascendencia jurídica, no puede identificarse, ya, en exclusiva, con el papel, como soporte, ni con la escritura, como unidad de significación. El ordenador y los ficheros que en él se almacenan constituyen, hoy día, una nueva forma de entender la materialidad de los títulos valores y, en especial, de los documentos… la admisión del documento electrónico es una realidad en nuestro ordenamiento, "sub conditione", sin embargo, de acreditar su autenticidad.* HERNÁNDEZ GUERRERO, F.J. y ALVAREZ DE LOS RIOS, J.L."Medios informáticos y proceso penal", en Estudios Jurídicos, Ministerio Fiscal IV, CEJAJ, Madrid, 1999, pág 580.

cual, a los efectos penales es documento *todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica.*

Es un concepto amplio, en tanto no sólo se considera como tal el papel como soporte tradicional, sino que da cabida a nuevos soportes tecnológicos o informáticos, como un video, fotos, CD, DVD, disco duro de un ordenador, USB, bases de datos, correo electrónico, mensaje SMS, etc. Surge así un paralelismo entre la prueba en soporte informático y el medio de prueba documental, pues mientras la prueba documental en soporte papel o similar hace presente el hecho controvertido al modo tradicional, la prueba en soporte electrónico se sustenta en un dispositivo de esa naturaleza, pero el hecho representado puede ser exactamente el mismo[528]. Dicho en otros términos, por documento a efectos de prueba se entiende tanto el electrónico como aquellos soportados en papel o similar, siempre y cuando se refieran, unos y otros, a los hechos controvertidos[529].

En este marco nos encontramos con el concepto de **"documento electrónico"** cuando la información se recoge en un soporte electrónico según un formato determinado y que sea susceptible de identificación y tratamiento diferenciado. En este sentido es necesario tener en cuenta la definición de documento electrónico que se contiene 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[530]: *"información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado"*[531].

---

[528] NIEVA FENOLL, J. La denomina atinadamente "*La prueba documental multimedia" vid.* NIEVA FENOLL, J. *Práctica y valoración de la prueba documental multimedia* en "Derecho y nuevas tecnología (Recurso electrónico".vol. II. Ed. Deusto, Bibao, 2011. págs. 53 a 72.

[529] SANCHÍS CRESPO, C. *La prueba en soporte electrónico* (…) ob. cit. pág. 713.

[530] SANCHÍS CRESPO, C. *La prueba en soporte electrónico* (…) ob. cit. pág 712. "*Esta ley no dedica ninguno de sus títulos a la regulación específica de la normativa probatoria, por lo que podría hacernos pensar que no afecta de modo directo a las fuentes de prueba y su acceso al proceso. Sin embargo, un análisis más detenido de su articulado va a revelarnos que algunos de los preceptos van a incidir de forma significativa en la normativa de los medios de prueba."*

[531] BOE núm. 160, de 6 de julio de 2011, páginas 71320 a 71348.

El documento electrónico[532] es "toda representación en forma electrónica de hechos jurídicamente relevantes, susceptibles de ser presentados en forma humanamente comprensible"[533], es decir, *el conjunto de datos electrónicos que representan los actos y negocios jurídicos, legibles mediante los correspondientes programas o sistemas lógicos y contenidos en discos o soportes magnéticos u ópticos que los almacenan*[534]. El documento electrónico posee unas características propias y diferenciadoras con respecto al documento tradicional, siendo la accesibilidad y la seguridad sus dos pilares fundamentales. Por ello y por su preservación a largo plazo el documento electrónico presenta un interés tanto jurídico, como técnico y archivístico[535].

Son tres los elementos que conforman la prueba informática:

A) Soporte material. Exige su lectura o traducción al lenguaje visual (desmaterialización del soporte y codificación del mensaje) lo que tiene el riesgo de la facilidad de copia y manipulación.

B) Contenido informativo: datos, hechos o narraciones, atribuible a una persona.

C) Relevancia jurídica: capaz de acreditar algún hecho con trascendencia jurídica.

---

[532]CASTILLEJO MANZANARES, R. "Hacia un nuevo proceso penal. Cambios necesarios". Ed. La Ley, Madrid, octubre 2010. En la Sección dedicada a los *Medios probatorios* recuerda que "es un documento electrónico un documento de texto, una hoja de cálculo, una imagen digitalizada, un fichero de sonido, un vídeo digitalizado o un registro o conjunto de registros dentro de una base de datos".

[533] Así lo recoge ALVAREZ CIENFUEGOS-SUAREZ, J.M."Los delitos de falsedad y los documentos generados electrónicamente. Concepto procesal y material de documento: nuevas técnicas", Cuadernos de Derecho Judicial, C.G.P.J., Madrid, 1993. pág. 8.

[534] ROVIRA DEL CANTO, E. "Tratamiento penal sustantivo de la falsificación informática". Cuadernos de derecho judicial nº 10, 2001 (ejemplar dedicado a internet y derecho penal). págs. 477 y 478.

[535] También el Artículo 27 Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, define el Documento judicial electrónico**.**
"1. Tendrán la consideración de documentos judiciales electrónicos las resoluciones y actuaciones que se generen en los sistemas de gestión procesal, así como toda información que tenga acceso de otra forma al expediente, cuando incorporen datos firmados electrónicamente en la forma prevista en la Sección 2.ª del Capítulo II del Título III de la presente Ley.
2. Las Administraciones competentes, en su relación de prestadores de servicios de certificación electrónica, especificarán aquellos que con carácter general estén admitidos para prestar servicios de sellado de tiempo.
3. Tendrá la consideración de documento público el documento electrónico que incluya la fecha electrónica y que incorpore la firma electrónica reconocida del secretario judicial, siempre que actúe en el ámbito de sus competencias, conforme a lo dispuesto en las leyes procesales".

Lo dicho permite poner de manifiesto de forma breve, pues se irán desarrollando en este capítulo, las diferencias de la prueba informática frente a otras pruebas en el proceso penal[536].

Un primer apunte sería que lo que ha de ser incorporado al proceso es todo aquel material (datos) que existe en formato electrónico o digital y que puede afectar a la prueba de los hechos objeto de enjuiciamiento, lo que incluye gigabytes de fotografías, videos, email, logs de chats y datos de sistema (internacionalmente se utiliza el término *electronic evidence*). Ello genera dificultades tanto para la obtención del dato relevante para la prueba (acceso al dispositivo o instrumento en el que físicamente se encuentra o a la red de comunicación donde se transmite), como para su incorporación al proceso a través de uno de los medios probatorios contemplados por la ley procesal.

Una segunda diferencia radica en que se precisa la utilización de un instrumento o dispositivo que posibilite la lectura del lenguaje binario. Es lo que se va a denominan dispositivos electrónicos, en los que se integran teléfonos móviles, equipos informáticos, instrumentos de almacenamiento de datos como DVD o dispositivos USB, tabletas, entre otros.

Y en tercer lugar, los datos pueden ser fácilmente modificados, sobreescritos o borrados, lo que determina un peligro evidente de manipulación de las pruebas. De esta forma resulta necesario utilizar técnicas que permitan obtener dichos datos y garantizar su autenticidad e integridad durante la tramitación del proceso.

[536] DELGADO MARTIN, J. "Investigación del entorno virtual (…) ob. cit. pág. 3.

2. REQUISITOS DE ADMISIBILIDAD DE LAS PRUEBAS INFORMÁTICAS: JUICIO DE LICITUD Y JUICIO DE FIABILIDAD.

Las introducción en el juicio de las pruebas informáticas requiere la comprobación de una serie de requisitos. Se ha hecho referencia a que la LECrim regula expresamente la forma y garantías que han de observarse para la práctica de las diligencias de investigación tecnológica con el fin de que su correcta obtención y tratamiento aseguren su ulterior valor como prueba al reunir los necesarios requisitos de validez sustancial, formal y procesal.

Como consecuencia de los actuales medios de investigación con los que cuentan los Jueces de Instrucción y las Fuerzas y Cuerpos de Seguridad del Estado para investigar los ciberdelitos, el resultado de estas diligencias debidamente reproducidos en el juicio oral pueden constituir una esencial prueba de cargo para los distintos encausados en numerosos procesos penales[537].

Por consiguiente, de su correcta adopción y práctica dependerá que el acusado pueda invocar o no el art. 11.1 LOPJ para poner de manifiesto la obtención de una prueba ilícita y conseguir que no pueda ser tenida en cuenta su valoración al tener que quedar excluida del material probatorio apto para enervar la presunción de inocencia[538].

Dado que la prueba debe practicarse con todas las garantías, se debe también comprobar si en el recorrido que siguen los elementos probatorios, desde su localización u obtención, hasta su incorporación al plenario, se han cumplido las exigencias normativas necesarias para garantizar su plena licitud, identidad e integridad[539].

---

[537] GONZÁLEZ-MONTES SÁNCHEZ, J.L. "Reflexiones sobre el Proyecto de Ley Orgánica de modificación de la LECrim para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas". Revista electrónica de ciencia penal y criminología nº 17-06. junio 2015, pág. 25.

[538] STS 300/2016, de 11 de abril; STS 511/2015, de 21 de julio; STS 747/2015 de 19 de noviembre; STS 113/2014, de 17 de febrero.

[539] VELASCO NÚÑEZ, E. "Novedades técnicas de investigación penal vinculadas a las nuevas tecnologías". El Derecho, Revista de Jurisprudencia nº 4, 24 de febrero de 2011. pág. 6.

Las pruebas informáticas están sometidas, en este sentido, a un doble juicio, a unos requisitos de admisibilidad[540].

Tales requisitos consisten de una parte, en un **previo juicio de licitud** (es decir, que la prueba se haya obtenido sin violar derechos fundamentales pues, en otro caso, sería nula, ex art. 11.1 LOPJ), y de otra, en un **juicio de fiabilidad,** que consiste en examinar la autenticidad (no manipulación)[541] y la integridad[542](conservación del contenido) del material aportado, la intangibilidad e inalterabilidad del mismo, y la ausencia de técnicas espurias en la obtención de la información recabada en el curso de tal medio de investigación, pues las dudas sobre la fiabilidad determinarán su inadmisibilidad probatoria.

De conformidad con el art. 230.2 LOPJ, resulta necesario asegurar la autenticidad (garantizar la fuente de la que proceden los datos) y la integridad (que el activo de información no ha sido alterado de manera no autorizada) de la prueba informática incorporada al proceso, de tal manera que quede garantizado que la sometida al tribunal de enjuiciamiento es la misma que la que fue incautada o aprehendida.

El juicio de fiabilidad determina, una serie de singularidades cuando se aplica a las pruebas informáticas. Y resultaría conveniente, como se verá, abordar estas singularidades a través de una regulación más precisa, para que se aporte más certidumbre a la actuación de los distintos sujetos del sistema penal y se reduzca el

---

[540] La distinción entre fiabilidad y licitud de la prueba es apuntada por CABEZUDO BAJO, M. J. *Fiabilidad y Licitud de la prueba de ADN en la UE y en España, "*El proceso penal en la Sociedad de la Información, nuevas tecnologías para investigar y probar el delito" (Pérez Gil, Coord). Ed. La Ley, Madrid 2012. (págs. 383-407). Si bien, el sentido que le atribuye esta autora no coincide con el que se recoge en el presente trabajo.

[541] 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, define:
Autenticación: *"Acreditación por medios electrónicos de la identidad de una persona o ente, del contenido de la voluntad expresada en sus operaciones, transacciones y documentos y de la integridad y autoría de estos últimos."*
Autenticidad: "*Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos".*

[542] 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, define Integridad como: *"Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada".*

margen error en sus actuaciones, limitando el riesgo de contaminación o alteración de la autenticidad e integridad de las pruebas.

2.1 Juicio de Licitud.

La admisibilidad de las pruebas informáticas en el proceso penal, al igual que la prueba en general, está condicionada a un previo juicio de licitud, es decir, que la prueba se haya obtenido sin violar derechos fundamentales, pues, en otro caso, sería nula (art. 11.1 LOPJ).

Además, la posible ilicitud se extendería también a las pruebas derivadas o reflejas, si entre ellas y las anuladas, existe una conexión natural o causal. En estos casos, la regla general es que todo elemento probatorio que pretenda deducirse a partir de un hecho vulnerador del derecho fundamental se haya también inmerso en la prohibición de valoración, siempre que se establezca un nexo entre unas y otras, que permita afirmar que la ilegitimidad constitucional de las primeras se extiende también a las segundas[543].

De ahí la importancia de que las diligencias de investigación tecnológicas, ya estudiadas, se hayan practicado con todas las garantías para que puedan servir como prueba en el acto del juicio oral, evitando la nulidad del material obtenido.

De forma esquemática, pues ya se desarrolló en profundidad en el capítulo anterior, se van a exponer los elementos necesarios que han de examinarse en el juicio de licitud, los requisitos que han de cumplirse para que la prueba no sea ilícita (2.1.A) Examinados estos requisitos, se pasará al estudio de las consecuencias de la falta de éstos (2.1.B).

[543] Conexión de antijuridicidad a la que se refieren entre otras las SSTS 300/2016, de 11 de abril; 511/2015, de 21 de julio; 747/2015 de 19 de noviembre; 113/2014, de 17 de febrero).

2.1.A) Requisitos para la licitud de la prueba:

- Requisitos comunes para interceptar comunicaciones telefónicas y telemáticas[544] y para incorporar datos electrónicos de tráfico o asociados:

    - La autorización del juez dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida[545].
    - Que se trate de los delitos del artículo 579.1 LECrim *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)* o cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación.

- Requisitos para el registro de dispositivos de almacenamiento de información (art. 588 sexies):
    - Autorización judicial que en función de lugar donde esté ubicado podrá ser:

        a) Dentro de un registro domiciliario: La resolución del juez de instrucción de entrada y registro habrá de extender su razonamiento a la justificación, en su caso, de las razones que legitiman el acceso de los agentes facultados a la información contenida en tales dispositivo.

        b) Fuera de un registro domiciliario: será necesario contar con autorización judicial en forma de auto motivado. Los efectos intervenidos, bien en sede judicial o fuera de ella, durante la investigación policial, quedarán como luego haremos

[544] Titulo VIII del Libro II de la Ley de Enjuiciamiento Criminal en los artículos 588 ter [a) - J)].

[545] Vid. Artículo 588 bis a. de la LECrim "*Principios rectores"*.

referencia precintados y a disposición de la Autoridad Judicial que, a iniciativa propia o petición de la Policía, o parte en el proceso, podrá solicitar un análisis pericial de la misma.

- Excepcionalmente, en casos de urgencia en que se aprecie un interés constitucional legítimo que haga imprescindible el acceso al contenido de los dispositivos, la Policía Judicial podrá llevar a cabo el examen directo de los datos contenidos en el dispositivo incautado, comunicándolo inmediatamente, dentro del plazo máximo de veinticuatro horas, por escrito motivado al juez competente, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado.
- No se exige investigar delito concreto para la adopción de esta medida.

- Requisitos para el registro remoto de equipos informáticos.

  - Autorización del Juez dictada con plena sujeción a los principios.

  - Siempre que persiga la investigación de alguno de los siguientes delitos del artículo 588 septies:
    - Delitos cometidos en el seno de organizaciones criminales.
    - Delitos de terrorismo.
    - Delitos cometidos contra menores o personas con capacidad modificada judicialmente.
    - Delitos contra la Constitución, de traición y relativos a la defensa nacional.
    - Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.

- Requisitos para el agente encubierto.
  - Autorización Judicial y
  - concreción respecto al catálogo delictual ya examinado anteriormente en el art. 282 bis 4 y 588 ter a LECrim.

2.1.B) Consecuencias de la falta de licitud.

En definitiva, si se practicaran estas diligencias de investigación tecnológica sin contar con los requisitos citados, ya sea sin la autorización judicial salvo los casos de urgencia, o que no se trate de la investigación de delitos concretos que legitiman su adopción, o bien que la autorización judicial no se ajuste a los principios que la fundamentan, la prueba sería nula por haber sido obtenida con violación del derecho a la intimidad personal del encausado o el secreto de las comunicaciones o la protección de datos según disponen los arts. 18.1, 18.3 y 18.4 de la Constitución Española (artículo 11.1 de la LOPJ) y carente de toda eficacia probatoria.

La sentencia no podrá fundamentarse en los datos obtenidos con estas diligencias ilícitamente practicadas, ni en dictámenes periciales (informáticos o similares), o declaraciones testificales que tengan por objeto los resultados de las mismas.

La conexión de antijuridicidad, también denominada *prohibición de valoración*, supone el establecimiento o determinación de un enlace jurídico entre una prueba y otra, de tal manera que, declarada la nulidad de la primera, se produce en la segunda una conexión que impide que pueda ser tenida en consideración por el Tribunal sentenciador a los efectos de enervar la presunción de inocencia del acusado.

Ahora bien, en la parte dedicada a la valoración de la prueba, se precisará con detalle hasta qué punto afecta esa nulidad al resto de pruebas incorporadas válidamente al proceso[546].

[546] Matiza en este sentido, la STS 768/2010, 15 de septiembre que acoge la STC 161/1999, 27 de septiembre [FJ 2] *"no significa que lo hallado en un registro verificado con vulneración del derecho a la inviolabilidad del domicilio haya de tenerse por inexistente en la realidad, ni tampoco que lo hallado no pueda ser incorporado de forma legítima al proceso por otros medios de prueba".*

2.2 Juicio de fiabilidad.

De manera específica, las pruebas informáticas deben estar sometidas a un juicio de fiabilidad, de modo que se debe comprobar la autenticidad e integridad de la información obtenida sin técnicas espurias y además contrastarla con la finalmente aportada en juicio.

En este juicio de fiabilidad se hace imprescindible garantizar lo que en otros delitos se denomina "cadena de custodia", para que no pueda apreciarse pérdida de eslabón alguno, con el fin de asegurar que aquello que se presenta ante los tribunales como prueba es lo mismo que se encontró en el escenario delictivo[547].

Pero el juicio de fiabilidad no solo se ciñe a la cadena de custodia sino que va más allá: pretende analizar la fiabilidad de todo el material probatorio, en el sentido de que la información, el dato, el archivo sobre el que ha de recaer la convicción judicial no venga viciado de inveracidad. En definitiva, se trata también de evitar la manipulación, los montajes fraudulentos, las confusiones, las falsedades, las imitaciones, distorsiones y las alteraciones del material informático objeto de prueba.

Dado que los datos electrónicos pueden modificarse fácilmente sin dejar rastros, ello entraña una pesada carga para las autoridades policiales, que deben reunir esas pruebas de acuerdo con procedimientos transparentes y seguros que les permitan establecer su autenticidad, integridad y confiabilidad[548]. A diferencia de la evidencia física, la evidencia digital presenta gran volatilidad y alta capacidad de manipulación. Por esta razón es importante aclarar que es indispensable verificar la autenticidad de las pruebas presentadas en medios digitales a diferencia de los no digitales, en los que la autenticidad de las pruebas aportadas no será refutada[549]. De ahí que no sea correcto utilizar la expresión cadena de custodia cuando se trata la prueba en los ciberdelitos, pues esos datos volátiles y manipulables difícilmente se pueden "custodiar".

---

[547] *Vid.* MESTRE DELGADO, E. *La cadena de custodia de los elementos probatorios obtenidos de dispositivos informáticos y electrónicos,* en "La cadena de custodia en el proceso penal", (AA.VV), edisofer, Madrid, 2015. págs. 49-50.

[548] ROVIRA DEL CANTO, E."Tratamiento penal sustantivo de (...)". ob. cit. págs. 477 y 478.

[549] MESTRE DELGADO, E. *La cadena de custodia de* (…) ob. cit. pág. 73.

Su viabilidad procesal está conectada a la autenticidad (no manipulación), a la integridad (conservación del contenido) y a la obtención sin técnicas espurias. Por ello, es importante el modo en que se incorporen. Se debe tener en cuenta en el juicio de fiabilidad en el momento de decidir sobre la admisibilidad del material probatorio:

- La autenticidad.
- Integridad, complitud o suficiencia.
- Confiabilidad.

Cualquier duda acerca de la fiabilidad del material de prueba determinará por lo general su inadmisibilidad. Las dudas del Juez sobre la concurrencia de estos requisitos serán determinantes para la denegación de la eficacia probatoria de los datos informáticos objeto de la prueba, pero a diferencia del juicio de licitud, las falta de fiabilidad no lleva consigo, por lo general, su nulidad.

Así, el Juez debe estar en condiciones de examinar la fiabilidad del proceso de copia o examinar la fiabilidad del registro del material de prueba, partiendo del portador original o del canal original de datos. También debe poder comprobar la fiabilidad del procedimiento de preservación y la seguridad de la propia preservación, de cualquier análisis de ese material y, en definitiva, si el material presentado ante el tribunal es conforme al material incautado y guardado originalmente.

Hay que ajustarse a los requisitos técnicos exigidos en todas y cada una de las diligencias de investigación practicadas. En eso consiste el juicio de fiabilidad: en comprobar que se han cumplido todas las prescripciones técnicas en la adopción de la medida y que el material aportado en juicio es el mismo que en su día se recogió sin tacha alguna en la investigación del delito.

Precisamente para garantizar la fiabilidad de las pruebas informáticas, la LECrim estable una serie de prescripciones técnicas que han de seguirse en la adopción de las medidas de investigación tecnológica. A saber:

2.2.A) *Requisitos técnicos para la captación del IMSI e IMEI.*

En el capítulo anterior se vio que la LECrim en el art. 588 ter l, habilita a la policía a valerse de "artificios técnicos" para acceder a los códigos tipo IMSI o IMEI de identificación del aparato de telecomunicaciones, sin necesidad de autorización judicial. Pero una vez obtenidos, sí es preceptiva la autorización judicial para conseguir del prestador de servicios, los datos asociados a esos códigos de identificación, como pueden ser los datos de abonado o tráfico, o para la practica de otras diligencias de investigación, como pudiera ser la intervención de las comunicaciones, registro remoto etc. La autorización judicial deberá especificar cuáles han sido "artificios técnicos" utilizados por la policía para la captación de esos códigos.

Cabe señalar que sin necesidad de recabar autorización judicial, se ha admitido el uso de unos simuladores conocidos como *"Cell Site Simulators"* para la captación de tales códigos emitidos por los terminales en la búsqueda de cobertura[550]. Sea cual sea el artificio utilizado en su obtención se habrá de hacer constar. Así lo recoge el art. 588 ter l, en su apartado segundo al señalar que *"la solicitud* (de la policía) *habrá de poner en conocimiento del órgano jurisdiccional la utilización de los artificios a que se refiere el apartado anterior.* Y posteriormente el auto que autorice la medida solicitada por la policía recogerá también cual ha sido el artificio técnico utilizado para la captación de tales códigos.

La concreción de qué tipo de artificio técnico ha sido empleado en la captación de dichos códigos deberá ser constatado como garantía en el juicio de fiabilidad de las pruebas informáticas, pues da transparencia a la actuación policial practicada y permite comprobar cómo se ha obtenido determinada información.

Lo mismo sucede respecto a la obtención del número de teléfono o identificación del titular.

[550] GIMENO BEVIÁ, J. "Análisis crítico de la reforma de la LECrim 2015 (…) ob. cit. pág. 10.

2.2.B) *Requisitos técnicos para incorporar datos electrónicos de tráfico o asociados.*

La LECrim no dedica ningún artículo al juicio de fiabilidad en la cesión de los datos de tráfico; tan solo dispone en el artículo 588 ter j que los datos electrónicos (…) solo podrán ser cedidos para su incorporación al proceso con autorización judicial. Por ello, hemos de acudir a la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, donde se dedica el artículo 6 a las normas generales sobre cesión de datos y el artículo 8 a la protección y seguridad de los datos, siendo ambos artículos claves en el juicio de fiabilidad de la cesión de datos electrónicos.

La Ley deja bastante libertad a la empresas prestadoras de servicios a la hora de fijar las condiciones que aseguren la autenticidad e integridad de los datos a entregar,[551] exige específicamente que las operadoras deberán identificar al personal especialmente autorizado para acceder a los datos, adoptar las medidas técnicas y organizativas que impidan su manipulación o uso para fines distintos de los comprendidos en la misma, su destrucción accidental o ilícita y su pérdida accidental, así como su almacenamiento, tratamiento, divulgación o acceso no autorizados[552].

Tales medidas de seguridad y garantías para la conservación, así como la supervisión de que se cumplan las previsiones a aplicar en tal tarea se rigen por las

[551] Sostiene el artículo 8 de la Ley de Conservación de datos que: "*1. Los sujetos obligados deberán identificar al personal especialmente autorizado para acceder a los datos objeto de esta Ley, adoptar las medidas técnicas y organizativas que impidan su manipulación o uso para fines distintos de los comprendidos en la misma, su destrucción accidental o ilícita y su pérdida accidental, así como su almacenamiento, tratamiento, divulgación o acceso no autorizados, con sujeción a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en su normativa de desarrollo.*
2. Las obligaciones relativas a las medidas para garantizar la calidad de los datos y la confidencialidad y seguridad en el tratamiento de los mismos serán las establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y su normativa de desarrollo.
3. El nivel de protección de los datos almacenados se determinará de conformidad con lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, y en su normativa de desarrollo.
4. La Agencia Española de Protección de Datos es la autoridad pública responsable de velar por el cumplimiento de las previsiones de la Ley Orgánica 15/1999, de 13 de diciembre, y de la normativa de desarrollo aplicables a los datos contemplados en la presente Ley".

disposiciones de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su Reglamento (Real Decreto 1720/2007, de 21 de diciembre)[553].

De otra parte, en cuanto el procedimiento de cesión de datos, tan solo dispone el artículo 6 de la Ley de Conservación de datos "*que la cesión de la información se efectuará mediante formato electrónico a los agentes facultados*". Será responsable en sede judicial de recoger los datos y documentarlos el LAJ (334 LECrim), testimoniando el soporte digital -CD o DVD, PEN- DRIVE-, pudiendo transcribirlos en papel, y al juicio oral se incorporaran a través de la lectura (730 LECrim), o el examen directo por el Juez (726 LECrim).

Habrá que tener en cuenta la Orden PRE/199/2013, de 29 de enero, por la que se define el formato de entrega de los datos conservados por los operadores de servicios de comunicaciones electrónicas o de redes públicas de comunicaciones a los agentes facultados (Ministerio de la Presidencia BOE núm. 40, de 15 de febrero de 2013).

2.2.C) *Requisitos técnicos para interceptar comunicaciones.*

La introducción del artículo 588 ter f LECrim es clave en el juicio de fiabilidad a la hora de adoptar la medida de interceptación de las comunicaciones, sean telefónicas o telemáticas, pues establece un control de la medida por parte del juez para asegurar la autenticidad e integridad de la información obtenida[554]. Y ello porque, como ya hemos

[553] El Real Decreto 1720/2007 obliga a que a estos datos se les apliquen las medidas de seguridad de nivel medio, entre las que se encuentran la designación del responsable del fichero que debe velar por las pautas de seguridad que se deben implementar, garantizar que sólo se puede acceder a dichos datos en los supuestos legalmente previstos y sólo por personal autorizado, la obligatoriedad de una auditoría sobre las medidas de seguridad aplicadas y su cumplimiento al menos cada dos años, el deber de registrar cada acceso o intento de acceso (fecha, hora y persona que lo hizo...), sólo la persona designada como responsable del fichero puede iniciar el procedimiento de recuperación de datos, y la destrucción y borrado de los datos cuando ya no exista obligación de retenerlos (artículos 81.4 y 95 y siguientes del Real Decreto 1720/2007). Las medidas de seguridad al detalle se pueden consultar en la guía de seguridad de datos elaborada por la Agencia Español de Protección de Datos https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_SEGURIDAD_2010.pdf

[554] Dice el precepto citado, bajo el título "Control de la medida".
"En cumplimiento de lo dispuesto en el artículo 588 bis g, la Policía Judicial pondrá a disposición del juez, con la periodicidad que este determine y en soportes digitales distintos, la transcripción de los pasajes que considere de interés y las grabaciones íntegras realizadas. Se indicará el origen y destino de

señalado, en aras a que la prueba sea considerada válida se deben respetar todas las garantías desde su obtención hasta la puesta a disposición judicial. De ahí, la necesidad expresamente establecida de indicar el origen y destino de la medida, así como el aseguramiento a través de establecer un sistema de sellado, o firma electrónica avanzado o sistema de adveración suficiente[555], entre otras.

El precepto introduce una serie de conceptos técnicos que conviene precisar, pues son la esencia del juicio de fiabilidad:

- Hace referencia a que *la transcripción de los pasajes que considere de interés y las grabaciones íntegras realizadas,* ***se entregará en soportes digitales distintos.***

El soporte digital es el material físico donde se almacenan los datos del dispositivo electrónico o sistema informático (por ejem. los discos magnéticos (disquetes, discos duros), los discos ópticos (CD, DVD), las cintas magnéticas, los discos magneto-ópticos (discos Zip, discos Jaz, SuperDisk), las tarjetas de memoria, etc).

Los soportes digitales utilizan el código binario para guardar la información en el medio físico, no siendo posible descifrar directamente la información que contienen. Ejemplo de esto es nuestra incapacidad para reconocer y descifrar a simple vista las marcas físicas con que se guarda la información en un CD. Por lo tanto, para poder consultar la información necesitamos un dispositivo mediador que la lea y decodifique.

El medio electrónico es el que decodifica la información contenida en los soportes digitales y nos presenta el tipo de medios para que podamos comprender e interpretar. Así, el estado de la información digital tiene una existencia completamente virtual, ya que solamente existe mientras el medio electrónico reproduce para nosotros los diferentes códigos que podemos descifrar, como son el texto, la imagen, el sonido y el video[556]. Por medio electrónico se entiende, el mecanismo, instalación, equipo o

---

cada una de ellas y se asegurará, mediante un sistema de sellado o firma electrónica avanzado o sistema de adveración suficientemente fiable, la autenticidad e integridad de la información volcada desde el ordenador central a los soportes digitales en que las comunicaciones hubieran sido grabadas".

[555] GIMENO BEVIÁ, J. "Análisis crítico de la reforma de la LECrim 2015 (…) ob. cit. pág. 10.

[556] http://www.revista.unam.mx/vol.6/num1/art05/art05_enero.pdf. En el soporte físico se guardan los archivos, de un formato u otro, en código binario. Lo que cambia entre ellos es la forma en que la

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[557].

El problema de los soportes digitales es su preservación a largo plazo o la propia conservación digital. Por ello, estos soportes digitales que entrega la policía al Juez y que contienen las grabaciones efectuadas, aunque la LECrim no dice nada al respecto, deberán cumplir las condiciones exigidas la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas[558] en el sentido en el que han de asegurar la identidad e integridad de la información necesaria para reproducirlo.

Se asegurará en todo caso la posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones, pues algunos formatos puede que dejen de ser legibles, por lo que deberán conservarse en formatos que aseguren la identidad e integridad de la información necesaria para reproducirlos. Y se ha de evitar la obsolescencia de los contenidos digitales mediante el uso de estándares abiertos que aseguren la legibilidad futura de los archivos contenidos en los soportes digitales. Por último, estos soportes digitales deberán contar con medidas de seguridad que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y

---

computadora interpreta y presenta el texto electrónico contenido en dichos archivos. Por lo mismo, en el caso que dos archivos de diferente formato contengan el mismo texto electrónico, su representación, al momento de visualizarlos en pantalla, será diferente. Por ejemplo: un archivo PDF presenta el texto formateado por paginación y es difícil de transformar, en cambio un archivo HTML para poder fragmentar la información debe de presentarla a través de varios archivos y comunicarlos con hipervínculos, o de otra manera tendrá que presentarse de continuo en una misma pantalla. Esta característica de la tecnología digital, que la información siempre tenga que ser interpretada antes de presentársele al usuario, provee una gran capacidad para desarrollar nuevos formatos en los que se innove la presentación e interactividad de la palabra escrita.

[557] *Vid.* 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.

[558]Antes regulado por Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, hasta que fue derogada, con efectos de 2 de octubre de 2016, por la disposición derogatoria única.2.b) de la Ley 39/2015, de 1 de octubre. Téngase en cuenta que la disposición final 7 de la citada ley establece un plazo de dos años desde su entrada en vigor para que produzcan efectos las previsiones relativas al registro electrónico de apoderamientos, registro electrónico, punto de acceso general electrónico de la Administración y archivo único electrónico, y por tanto, hasta ese momento, se mantendrán en vigor los artículos de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, que traten sobre las materias citadas.

conservación de los documentos almacenados[559].

Respecto a estos soportes digitales, la STS 1215/2009, de 30 de diciembre, se refiere a ellos en relación al sistema SITEL al analizar la naturaleza jurídica de la información que se facilita por el agente a la autoridad judicial a través de soportes físicos, así como la forma en que ha de hacerse valer la prueba en juicio, en especial cuando ha tenido lugar alguna tacha formal.

La referida sentencia considera que los soportes físicos en los que se trasladan a la autoridad judicial las informaciones recabadas con motivo de la interceptación de comunicaciones participan de la naturaleza de documento público, digitalizado, se sobreentiende; y ello por las mismas razones por las que la jurisprudencia anterior de la misma Sala Segunda confería tal valor de documento público a las cintas magnetofónicas originales donde se almacenaban las conversaciones objeto de intervención. Como quiera que el art. 318 de la Ley de Enjuiciamiento Civil permite la aportación a juicio de documentos públicos a través de soportes digitales, sin perjuicio de la posible impugnación de su autenticidad, la sentencia establece también que los CD y DVD en los que se trasmite al juez el resultado de la labor de intervención de comunicaciones acordada gozan de presunción de autenticidad, salvo prueba en contrario. Es decir: "*El sistema de escuchas telefónicas, que se plasma en un documento oficial obtenido con autorización judicial y autenticado su contenido por la fe pública judicial goza de valor probatorio, salvo que mediante pericia contradictoria se demuestre la falsedad o alteración de las conversaciones grabadas*"(STS 1215/2009, de 30 de diciembre [FJ 1º apt. c.17].

Siguiendo con el análisis del artículo 588 ter f, la expresión *"distintos*" que contiene el precepto en referencia a los soportes digitales se entiende no en relación al

[559] Antes se recogía en el Artículo 31 de la Ley11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Ahora en el Artículo 17 de la Ley 39/2015, de 1 de octubre.
"2. Los documentos electrónicos deberán conservarse en un formato que permita garantizar la autenticidad, integridad y conservación del documento, así como su consulta con independencia del tiempo transcurrido desde su emisión. Se asegurará en todo caso la posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones. La eliminación de dichos documentos deberá ser autorizada de acuerdo a lo dispuesto en la normativa aplicable.
3. Los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad, de acuerdo con lo previsto en el Esquema Nacional de Seguridad, que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos, así como el cumplimiento de las garantías previstas en la legislación de protección de datos".

formato utilizado, sino a que cada entrega se hará en un soporte distinto al aportado anteriormente. Con ello se posibilita que mientras que el acto de injerencia se desarrolla el Juez esté permanentemente informado de la evolución y vicisitudes de la ejecución de la medida con cada una de las entregas.

En el caso de que se entreguen para facilitar la tarea del juez, las transcripciones parciales de los pasajes que la policía judicial considere de interés, han de hacerse en soportes independientes de las grabaciones íntegras realizadas. Se muestra con ello de este modo un especial interés en que el soporte original de la grabación se encuentre desde un principio libre de cualquier sospecha de manipulación o acceso inconsentido.

Pese a que la norma no establezca sanción específica para el supuesto de incumplimientos relacionados con la entrega de grabaciones, transcripciones o informes de dación de cuenta, debe considerarse aplicable la jurisprudencia que considera la existencia de meras irregularidades no invalidantes de la injerencia en aquellos supuestos en que podemos hablar de retrasos que no impiden o dificultan seriamente la capacidad de control de la fase de ejecución de la medida por parte del Juez autorizante.

- En segundo lugar, el precepto exige también dentro del juicio de fiabilidad que ***se indique el origen y destino de cada una de ellas.***

De tal modo, que se aporte junto con la grabación de las conversaciones la identificación de los terminales que contactan entre sí o el origen y destino de cada una de las conversaciones grabadas, como medio de asegurar la autenticidad e integridad de la información obtenida en el proceso de interceptación.

- En tercer lugar, dispone el precepto que **se asegurará** la autenticidad e integridad de la información volcada desde el ordenador central a los soportes digitales en que las comunicaciones hubieran sido grabadas mediante los siguientes métodos:

- un sistema de sellado
- o firma electrónica avanzado
- o sistema de adveración suficientemente fiable.

a) SISTEMA DE SELLADO: Es un mecanismo que permite demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el

tiempo. El uso de un sistema de sellado de tiempo aparece como indispensable para mantener la validez de los documentos a lo largo de los años y proporciona un valor añadido a la utilización de firma digital ya que ésta por sí sola no proporciona ninguna información acerca del momento de creación de la firma. El sellado de tiempo lo definía la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos[560] como: *Acreditación a cargo de un tercero de confianza de la fecha y hora de realización de cualquier operación o transacción por medios electrónicos.*

b) FIRMA ELECTRÓNICA: es el conjunto de datos en forma electrónica consignados junto a otros o asociados con ellos que pueden ser utilizados como medio de identificación del firmante[561].

La firma electrónica se basa en la criptografía de claves asimétricas generadas informáticamente, una de las cuales, denominada clave privada, sólo es conocida por su titular; otra, la denominada clave pública se da a conocer a las Entidades de Certificación que van a garantizar la autenticidad de la firma digital al ser las detentadoras de los registros de claves públicas. Con la clave pública el receptor del mensaje desencripta su contenido y constata que ha sido encriptado por quien poseía la clave privada (así puede comprobar la identidad del emisor y la autenticidad del mensaje). Para activar la firma electrónica se dispone de un soporte o tarjeta de identificación electrónica,

[560] Norma derogada, con efectos de 2 de octubre de 2016, por la disposición derogatoria única.2.b) de la Ley 39/2015, de 1 de octubre. Téngase en cuenta que la disposición final 7 de la citada ley establece un plazo de dos años desde su entrada en vigor para que produzcan efectos las previsiones relativas al registro electrónico de apoderamientos, registro electrónico, punto de acceso general electrónico de la Administración y archivo único electrónico, y por tanto, hasta ese momento, se mantendrán en vigor los artículos de la presente ley que traten sobre las materias citadas.

[561] Dentro de la firma electrónica, conforme a la Ley 59/2003, de 19 de diciembre, de firma electrónica, se distingue entre:
- Firma electrónica: Según el apartado 1 del artículo 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.
- Firma electrónica avanzada: Según el apartado 2 del artículo 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, la firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede utilizar, con un alto nivel de confianza, bajo su exclusivo control.
- Firma electrónica reconocida: Según el apartado 3 del artículo 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.
- Sistema de firma electrónica: Conjunto de elementos intervinientes en la creación de una firma electrónica. En el caso de la firma electrónica basada en certificado electrónico, componen el sistema, al menos, el certificado electrónico, el soporte, el lector, la aplicación de firma utilizada y el sistema de interpretación y verificación utilizado por el receptor del documento firmado.

accesible mediante la introducción del correspondiente número de identificación personal.

La firma electrónica avala que el mensaje no ha sido alterado o modificado (respeto a la integridad); impide que se acceda al mensaje o documento de forma inconsentida (confidencialidad); y hace que una vez aceptado no pueda ser rechazado sin que exista pacto de retracción o desistimiento (función de no repudiación). Ahora bien, la firma electrónica identifica al titular de la clave pero no al firmante, que puede ser una persona distinta. La firma electrónica avanzada garantiza la identidad del firmante e integridad del mensaje, salvo que se demuestre lo contrario[562]. Y firma electrónica reconocida es la avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma y tiene el mismo valor que la firma manuscrita en relación con los datos consignados en papel[563].

No obstante, la firma digital no está exenta de problemas, como los que pueden surgir en relación a la identidad del firmante y a su validez temporal. Como sostiene algún autor[564] en realidad la firma digital sólo prueba que se utilizó la clave privada del sujeto y no, sin embargo, el acto personal de la firma. Esto sucede a diferencia de la firma autógrafa que consiste en una biometría y, por tanto, siendo auténtica, confirma el acto personal de la firma. De manera que no existiría una necesaria coincidencia entre presencia de la correcta firma digital y la voluntad real de firma del titular de la clave privada. Se presenta un problema entonces de autoría real de la firma electrónica con una posible falsedad en la misma, pero a diferencia de la firma manuscrita que requeriría de un dictamen pericial caligráfico, la falsedad de la firma electrónica debería investigarse con técnicas distintas, que persiguiesen básicamente que el supuesto firmante (titular de la firma electrónica avanzada) no se encontraba en el lugar desde el

[562] Podría ser el caso de suplantación de la personalidad o vicio de consentimiento, al disponer de la firma de otro por sustracción o utilización de la clave por negligencia del titular que es robado o engañado.

[563] Dirección de Sistemas de Información Departamento Ceres. Firma Electrónica De Larga Duración. Firma Longeva. Editado por CERES, en 2008. http://www.cert.fnmt.es/documents/11601/94960/Firmas_longevas.pdf/1461fea7-64a8-4b27-8cdd-9f31f40f5f0c

[564] HERNÁNDEZ GUERRERO, F.J. y ALVAREZ DE LOS RIOS, J.L.: "Medios informáticos y (...)". ob. cit. págs. 583 y 584.

cual se realizó la firma[565]. Dicho terminal es fácil de identificar por constancia de la IP del dispositivo desde el que se ha firmado, por lo que demostrar la falsedad de la firma digital, no parece revestir a priori una excesiva complejidad dada la multitud de sistemas incluso de uso personal que permiten la localización de un individuo prácticamente de forma constante.

Otro problema[566] es que las claves empleadas en la firma digital tienen asignadas de forma anticipada un periodo temporal de validez, durante el que su empleo resulta legítimo y produce todos los efectos legalmente previstos, lo que conlleva la problemática de la comprobación de la autenticidad de las ya realizadas mientras el certificado estaba vigente, una vez deja de estarlo, sea porque se ha acabado el plazo de vigencia de la clave o porque se haya revocado por anticipado, bien voluntariamente bien por la pérdida de la clave. Para solucionar este inconveniente se precisa incorporar a la firma electrónica los elementos de tiempo y validación que permitan verificar esa firma sin ayuda externa, se deberán guardar y mantener todas las evidencias que posibilitarán su verificación posterior. Existen distintos formatos de firma que van incrementando la calidad de la misma hasta conseguir una firma que pueda ser verificada a largo plazo (de forma indefinida) con plenas garantías jurídicas[567].

---

[565] NIEVA FENOLL, J. "Práctica y valoración de la prueba documental multimedia". Actualidad civil nº 17, 2009, págs. 5 y 6. Considera que a efectos procesales la firma manuscrita es más segura que la electrónica. La ventaja de la firma manuscrita es que la misma goza de la característica de la intransferibilidad. Sin embargo, esa misma garantía no existe en absoluto con la firma electrónica avanzada, reconocida o no, porque la misma es perfectamente transferible ya que cualquiera puede comunicar sus claves a otra persona. En definitiva, el uso indebido de una firma manuscrita siempre deja rastro, y el de una firma electrónica, incluso con las máximas garantías, podría no dejarlo, o no ser posible averiguar dicho rastro.

[566] Dirección de Sistemas de Información Departamento Ceres. Firma Electrónica De Larga Duración. Firma Longeva. Editado por CERES, en 2008. http://www.cert.fnmt.es/documents/11601/94960/Firmas_longevas.pdf/1461fea7-64a8-4b27-8cdd-9f31f40f5f0c . Es posible que una firma no pueda repetirse años después de su generación y con el paso del tiempo, las claves, los algoritmos empleados, etc, se pueden considerar obsoletos o incluso podemos no tener acceso a determinados datos necesarios para la comprobación.

[567] Dirección de Sistemas de Información Departamento Ceres. Firma Electrónica De Larga Duración. Firma Longeva. Editado por CERES, en 2008. http://www.cert.fnmt.es/documents/11601/94960/Firmas_longevas.pdf/1461fea7-64a8-4b27-8cdd-9f31f40f5f0c. *Distintos formatos de firma que van incrementando la calidad de la misma hasta conseguir una firma que pueda ser verificada a largo plazo (de forma indefinida) con plenas garantías jurídicas:*

1. Firma Básica (AdES BES), firma básica para satisfacer los requisitos de la firma electrónica avanzada.
2. AdES T, se añade un sellado de tiempo (TimeStamp) con el fin de situar en el tiempo el instante en que se firma un documento.

En definitiva, en la actualidad, la firma electrónica se constituye en el mayor elemento acreditativo de la ausencia de vulnerabilidad de los documentos contenidos y transmitidos en redes informáticas, con la consecuente relevancia en el ámbito probatorio del documento electrónico en el proceso penal.

Así lo reconocen las sentencias del Tribunal Supremo (STS 544/2011, de 7 de junio, STS 554/2012, de 4 de julio, STS 722/2012, de 2 de octubre y STS 143/2013, de 28 de febrero, STS 138/2015, de 13 de marzo, entre otras) al considerar a la firma electrónica como paradigma de garantía de autenticidad e inalterabilidad. Ello viene reforzado por las conclusiones que la Agencia Española de Protección de Datos hizo en su informe sobre la inspección del sistema SITEL, publicadas el 19 de enero de 2010,[568] que afirmó de forma tajante que: "*Se considera que los procedimientos de firma electrónica implantados en el momento en que la información se incorpora al sistema, su grabación en otros soportes y su transmisión a la autoridad judicial, garantizan los principios de exactitud e integridad previstos en la LOPD"*

Conforme a lo dispuesto en la Ley 59/2003, de 19 de diciembre[569], únicamente el sistema denominado de firma electrónica reconocida se equipara funcionalmente a la firma manuscrita, y posee, por tanto, la misma eficacia jurídica que aquella[570], lo cual no obsta para que otras firmas digitales distintas de la reconocida pudieran tener tengan eficacia jurídica y probatoria.

La LECrim exige la firma electrónica avanzada a pesar de las reticencias que puede suscitar que se exija la firma avanzada y no la reconocida.

---

3. AdES C, añade un conjunto de referencias a los certificados de la cadena de certificación y su estado, como base para una verificación longeva.
4. AdES X, añade sellos de tiempo a las referencias creadas en el paso anterior.
5. AdES XL, añade los certificados y la información de revocación de los mismos, para su validación a largo plazo.
6. AdES A, permite la adición de sellos de tiempo periódicos para garantizar la integridad de la firma archivada o guardada para futuras verificaciones.

Se ha conseguido una firma longeva "autoverificable" con el paso del tiempo.

[568] *Vid.* RODRÍGUEZ LAÍNZ, J L. "Análisis del espectro electromagnético de señales inalámbricas (…)". ob. cit. pág 26.

[569] Según la exposición de motivos de la Ley.

[570] Art. 4 de la Ley 59/2003.

Hay que traer a colación el artículo 14 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[571], donde precisamente se hace referencia las formas de identificación y autenticación mediante la firma electrónica, incluyendo a cualquiera que resulte adecuado para garantizar la identificación de los firmantes y, en su caso, la autenticidad e integridad de los documentos electrónicos incluyendo a la firma avanzada[572] y también el artículo 10 de la Ley 39/2015 que regula los Sistemas de firma admitidos por las Administraciones Públicas[573] admitiendo la reconocida y la avanzada.

[571]Art. 14 de la Ley 18/2011

1. La Administración de Justicia admitirá, en sus relaciones por medios electrónicos, sistemas de firma electrónica que sean conformes a lo establecido en la Ley 59/2003, de 19 de diciembre, de firma electrónica, y resulten adecuados para garantizar la identificación de los firmantes y, en su caso, la autenticidad e integridad de los documentos electrónicos.

2. Sin perjuicio de lo dispuesto en los artículos 4 y 6 de la presente Ley y en todo caso, con sujeción estricta a lo dispuesto por las leyes procesales, los ciudadanos y profesionales del ámbito de la Justicia podrán utilizar los siguientes sistemas de firma electrónica para relacionarse con la Administración de Justicia:

a. Los sistemas de firma electrónica incorporados al Documento Nacional de Identidad, para personas físicas.

b. Sistemas de firma electrónica avanzada, incluyendo los basados en certificado electrónico reconocido, admitidos por las Administraciones públicas.

c. Otros sistemas de firma electrónica, como la utilización de claves concertadas en un registro previo como usuario, la aportación de información conocida por ambas partes u otros sistemas no criptográficos, en los términos y condiciones que en cada caso se determinen.

3. La Administración de Justicia podrá utilizar los siguientes sistemas para su identificación electrónica y para la autenticación de los documentos electrónicos que produzca:

a. Sistemas de firma electrónica basados en la utilización de certificados de dispositivo seguro o medio equivalente que permita identificar la sede judicial electrónica y el establecimiento con ella de comunicaciones seguras.

b. Sistemas de firma electrónica para la actuación judicial automatizada.

c. Firma electrónica del personal al servicio de la Administración de Justicia.

d. Sistemas de intercambio electrónico de datos en entornos cerrados de comunicación, conforme a lo que específicamente se haya convenido.

[572] También lo recogía la Ley 11/2007, aunque ya derogada, en su artículo 35. "Los interesados podrán aportar al expediente copias digitalizadas de los documentos, cuya fidelidad garantizarán mediante firma electrónica avanzada".

[573]Art. 10 de la Ley 39/2015

"1. Los interesados podrán firmar a través de cualquier medio que permita acreditar la autenticidad de la expresión de su voluntad y consentimiento, así como la integridad e inalterabilidad del documento.

2. En el caso de que los interesados optaran por relacionarse con las Administraciones Públicas a través de medios electrónicos, se considerarán válidos a efectos de firma:

a) Sistemas de firma electrónica reconocida o cualificada y avanzada basados en certificados electrónicos reconocidos o cualificados de firma electrónica expedidos por prestadores incluidos en la "Lista de confianza de prestadores de servicios de certificación". A estos efectos, se entienden comprendidos entre los citados certificados electrónicos reconocidos o cualificados los de persona jurídica y de entidad sin personalidad jurídica.

b) Sistemas de sello electrónico reconocido o cualificado y de sello electrónico avanzado basados en certificados electrónicos reconocidos o cualificados de sello electrónico incluidos en la «Lista de confianza de prestadores de servicios de certificación".

En mi opinión, el debate sobre firma reconocida o avanzada no merece discusión alguna, siempre y cuando el sistema de firma utilizado sea expedido por prestadores incluidos en la Lista de confianza de prestadores de servicios de certificación[574] y garantice la identificación de los firmantes, así como la autenticidad e integridad de los documentos electrónico, pues con estos presupuestos el sistema de firma usado cumple las exigencias del juicio de fiabilidad.

c) SISTEMA DE ADVERACIÓN SUFICIENTEMENTE FIABLE: por último, introduce el precepto dentro del juicio de fiabilidad, y como herramienta de garantía de la autenticidad e inalterabilidad del contenido de las grabaciones, el nuevo concepto de *sistema de adveración suficientemente fiable,* como cláusula abierta a la evolución de las posibilidades tecnológicas[575]. Se trata del establecimiento de un sistema que las nuevas tecnologías en un futuro puedan permitir y que garantice, cuando menos, y conforme a lo apuntado para la firma electrónica, la integridad de cualquier información suministrada, para que se pueda atribuir plena eficacia probatoria.

En conclusión, mediante el artículo 588 ter f de la LECrim desaparece el riesgo de alterabilidad de contenidos en el traslado de la información a los soportes

---

c) Cualquier otro sistema que las Administraciones Públicas consideren válido, en los términos y condiciones que se establezcan.
Cada Administración Pública, Organismo o Entidad podrá determinar si sólo admite algunos de estos sistemas para realizar determinados trámites o procedimientos de su ámbito de competencia.
3. Cuando así lo disponga expresamente la normativa reguladora aplicable, las Administraciones Públicas podrán admitir los sistemas de identificación contemplados en esta Ley como sistema de firma cuando permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados.
4. Cuando los interesados utilicen un sistema de firma de los previstos en este artículo, su identidad se entenderá ya acreditada mediante el propio acto de la firma".

[574]Con arreglo a la Directiva 2006/123/CE del Parlamento Europeo y el Consejo relativa a los servicios en el mercado interior, se prevé que cada Estado miembro de la UE publique una «Lista de confianza» que contenga una información mínima referente a los prestadores de servicios de certificación que expidan certificados reconocidos al público supervisados en ese Estado. Esta Lista debe cumplir las especificaciones técnicas recogidas en el Anexo de la Decisión de ejecución de la Comisión 2013/662/UE de 14 de octubre de 2013, por la que se modifica la Decisión 2009/767/CE en lo relativo al establecimiento, el mantenimiento y la publicación de listas de confianza de proveedores de servicios de certificación supervisados o acreditados por los Estados Miembros. El Ministerio de Industria, Energía y Turismo ha elaborado una Lista de confianza de prestadores de servicios de certificación (TSL) correspondiente a los prestadores que expiden certificados reconocidos y que están establecidos y supervisados en España, Fecha de última actualización: 19/01/2016.
https://sede.minetur.gob.es/Prestadores/TSL/TSL.pdf 25/2/2016 a las 14.07 horas.

[575] RODRÍGUEZ LAINZ, J. L. "La interceptación de las comunicaciones telefónicas y telemáticas en el Anteproyecto (…)". ob. cit. pág. 11.

informáticos (CD o DVD) que se facilitan a la autoridad judicial, pues con estas certificaciones se garantiza:

a) que desde el momento en que culminó el proceso de transferencia de archivos hasta su recepción por el Juzgado, ese soporte informático (DVD o CD) no ha sido abierto.

b) Que, en consecuencia, no ha existido riesgo de manipulación.

c) Que quien garantiza la integridad del documento es el funcionario responsable del tratamiento y, por tanto, el único con capacidad de autentificación.

Solo los soportes entregados a la autoridad judicial que cuenten con la garantía de sistema de sellado o de firma electrónica avanzada o de sistema de adveración suficientemente fiable estará a salvo su integridad y autenticidad, por lo que sería difícil que pudiera prosperar una impugnación por falta de fiabilidad. En caso de impugnación se afirma[576] que no bastaría con una impugnación genérica, un mero alegato de irregularidades en el tratamiento, conservación o transmisión de la información almacenada a la autoridad judicial para desvirtuar el referido documento electrónico. Habrá de hacerse una impugnación mínimamente razonada y razonable en la que se dé cuenta de por qué se considera que ha existido manipulación o riesgo de manipulación. A tal efecto sería de aplicación artículo 8 de la ley 59/2003, de 19 de diciembre de firma electrónica[577] y los artículos 326.3, 382.2 y 384.1 y 2 de la LEC[578].

[576] RODRÍGUEZ LAINZ, J. L. "La interceptación de las comunicaciones telefónicas y telemáticas en el Anteproyecto (…) "ob. cit. pág. 11.

[577] Art. 8 de la ley 59/2003, de 19 de diciembre de firma electrónica *"Si se impugnare la autenticidad de la firma electrónica reconocida con la que se hayan firmado los datos incorporados al documento electrónico se procederá a comprobar que se trata de una firma electrónica avanzada basada en un certificado reconocido, que cumple todos los requisitos y condiciones establecidos en esta Ley para este tipo de certificados, así como que la firma se ha generado mediante un dispositivo seguro de creación de firma electrónica.*
La carga de realizar las citadas comprobaciones corresponderá a quien haya presentado el documento electrónico firmado con firma electrónica reconocida. Si dichas comprobaciones obtienen un resultado positivo, se presumirá la autenticidad de la firma electrónica reconocida con la que se haya firmado dicho documento electrónico siendo las costas, gastos y derechos que origine la comprobación exclusivamente a cargo de quien hubiese formulado la impugnación. Si, a juicio del tribunal, la impugnación hubiese sido temeraria, podrá imponerle, además, una multa de 120 a 600 euros.
Si se impugna la autenticidad de la firma electrónica avanzada, con la que se hayan firmado los datos incorporados al documento electrónico, se estará a lo establecido en el apartado 2 del artículo 326 de la Ley de Enjuiciamiento Civil".

- Pero, ¿qué sucedería en aquellos casos en los que el soporte no cuente con estas garantías? En términos generales, la firma electrónica no es sino un método más de autenticación de la identidad del emisor. La remisión o entrega a la autoridad judicial del soporte electrónico que contiene la información objeto de interceptación, la sola entrega del soporte por el funcionario policial sin ningún sistema de sellado, firma electrónica o sistema de adveración, no cumpliría con ese primer nivel de autenticación al que responderían estos sistemas. Ante la ausencia de tales certificaciones, aunque haya sido por olvido o error sin que medie manipulación alguna, la información facilitada a la autoridad judicial por la policía se mostraría vulnerable a impugnaciones de las defensas, y la falta de fiabilidad alcanzaría al contenido del documento así como a su autenticidad e integridad[579]. En definitiva, en estos casos es probable que no superase el juicio de fiabilidad exigible para su admisión como prueba, existiendo fundadas y poderosas razones para su rechazo como elemento probatorio.

Por último, el artículo 588 ter f. Dispone que: Se asegurará *la autenticidad e integridad de la* ***información volcada desde el ordenador central a los soportes digitales*** *en que las comunicaciones hubieran sido grabadas.*

La LECrim no hace referencia alguna al medio empleado para captar las comunicaciones telemáticas, pero parece que se diseña un sistema con miras al sistema SITEL, en el que la intervención de una unidad u ordenador central se convierte en

[578] Podría entrar en juego en estos casos las normas de impugnación previstas en tales supuestos en la Ley de Enjuiciamiento Civil para la aportación de prueba documental, documentos electrónicos o archivos de audio o vídeo. Los clásicos documentos públicos o privados cuentan con su régimen propio de impugnación -arts. 320.2 y 326 LEC-, consistentes en su cotejo con original en el primer caso, y pruebas periciales sobre autenticidad o inalterabilidad del documento en el segundo supuesto; los arts. 326.3, 382.2 y 384.1 y 2, permiten ese mismo juego de periciales para la impugnación o acreditación de la autenticidad o inalterabilidad del documento o archivo electrónico, con contenidos de datos electrónicos o simples archivos de audio o vídeo, dando de este modo cobertura legal a la posibilidad de contradecir las razones de la impugnación, bien como prueba anticipada, bien mediante su preparación para su práctica en el acto del juicio oral. No obstante, lo cierto es que la LEC no exige ningún fundamento de la impugnación. Basta con que el impugnante manifieste que impugna la autenticidad del documento para que, automáticamente y por éste simple hecho, el documento, si es privado, ya no haga fe en los términos del artículo 319 LEC (art. 326 LEC) y si es público, éste ya no hace prueba plena en los términos del artículo 319 de la LEC (art. 320 LEC). Producida por tanto la impugnación, se deja en manos de la parte impugnada la posibilidad de proponer prueba sobre su autenticidad, si el documento es privado (art. 326 LEC) y sin perjuicio de la posibilidad de valoración de la prueba conforme a los criterios de la sana crítica (art.326 LEC) y, si es público, se procede de la forma que determina el artículo 320 de la LEC.

[579] RODRÍGUEZ LAÍNZ, J. L. "De vueltas con SITEL". Diario La Ley nº 7515, sección doctrina, 2010 pág. 11. "*El soporte físico carecería de una certificación oficial afectante no solo a la autenticidad del documento electrónico, sino al respeto de las garantías de intangibilidad, complitud e inalterabilidad, exigibles para la conservación y transmisión de la información almacenada en el centro de recepción".*

clave del esquema. Al permitir el propio texto legal otras vías de interceptación, distintas de la telefónicas, debería haberse añadido una cláusula que permitiera su adaptación a estos otros procedimientos de interceptación que en un futuro se puedan implantar, imponiendo reglas o garantías mínimas para su llevanza, con la correspondiente reglamentación de la incorporación de la información al proceso[580]. El uso de programas de captación de las comunicaciones telemáticas por la policía, similar a SITEL, pero que permitan la captación de las diversas formas de comunicación, sin intervención de un operador de comunicaciones electrónicas convertiría al agente facultado en garante exclusivo de la ejecución de la medida. Ello conllevaría que, bajo su responsabilidad, se arbitren herramientas que puedan garantizar la autenticidad e inalterabilidad de toda la información que se recabe en el curso de una injerencia concreta.

Lo que se hace preciso para cualquier sistema de interceptación de comunicaciones telemáticas, es la salvaguardia de una información original ajena a cualquier riesgo de manipulación o acceso inconsentido que pudiera generar una duda razonable sobre la alteración de lo que se conserva. Cualquier medida de esta naturaleza debería partir de la habilitación de un soporte de almacenamiento que, sometido a estrictas medidas de seguridad de un nivel alto similar al exigido para SITEL[581], permitiera realizar un seguimiento sobre todas las vicisitudes que hubieran acontecido durante su captación y conservación (restricción y registro de control de accesos, conservación a disposición de la autoridad judicial,...). Debería contar con medidas de seguridad tendentes a la evitación de manipulaciones en cuanto a la realización de copias destinadas al tratamiento de la información almacenada o su facilitación a la autoridad judicial, del tipo firma electrónica, como la empleada igualmente para SITEL, así como garantizar la destrucción del material almacenado, una vez cubierta la finalidad para la cual se llevó a efecto el acto de injerencia[582] .

---

[580] RODRÍGUEZ LAINZ, J. L. "La interceptación de las comunicaciones telefónicas y telemáticas en el Anteproyecto (…)" ob. cit. pág. 12.

[581] *Vid*. arts. 81, en sus apartados 1,b y 3.b, y 101.1 del Real Decreto 1720/2007, de 21 de diciembre por el que se aprueba el Reglamento que desarrolla la Ley de Protección de Datos. RODRÍGUEZ LAÍNZ, J L. "Análisis del espectro electromagnético de señales inalámbricas (…) ob. cit. pág. 26.

[582] RODRÍGUEZ LAÍNZ, J L. "Análisis del espectro electromagnético de señales inalámbricas (…)". ob. cit. pág. 19.

En los nuevos procedimientos para practicar interceptaciones telemáticas pueden surgir dudas referentes al método de conservación y custodia del material objeto de interceptación. Por lo que se debe establecer la necesidad de poder posibilitar el cotejo y control de autenticidad, inalterabilidad e integridad del material que, en soporte electrónico, se facilite a la autoridad judicial a través del agente facultado[583].

Ahora bien, pueden surgir dudas respecto de la autenticidad e integridad de la información volcada desde el ordenador central a los soportes digitales en que las comunicaciones hubieran sido grabadas, pues esta información ha podido ser manipulada antes incluso de ser garantizada mediante el sistema de sellado, firma electrónica avanzado o sistema de adveración suficientemente fiable, o incluso antes de ser volcada desde el ordenador central. Se trata de acreditar que la información facilitada no haya sido objeto de posible manipulación, bien por modificación de contenidos o datos, bien por eliminación. En ese sentido hay que contar con un sistema de interceptación de las comunicaciones que técnicamente impida realizar modificación o eliminación o borrado alguno, o que, en caso de ser ello posible, quede en el sistema informático un rastro electrónico que permita constatar tal eventualidad y su autoría. Precisamente, el informe de inspección de la AEPD asegura la inalterabilidad de los ficheros de SITEL, lo que comporta el cumplimiento del nivel alto de protección en lo referente a la garantía de inalterabilidad de la información y control de accesos[584].

La STS 1215/2009, de 30 de diciembre, en relación a SITEL[585] se muestra decididamente complaciente con el sistema al que califica de *sistema de grabación de alta seguridad y de difícil o, por no decir imposible, manipulación sin que la persona que la realice sea detectada por su clave y personalmente identificada con mayor seguridad que en un sistema tradicional de cintas analógicas"*[586].

---

[583] RODRÍGUEZ LAÍNZ, J. L. "De vueltas con SITEL". ob. cit. pág. 1.

[584] El informe de la AEPD asegura que el sistema SITEL, a nivel de centros de recepción, garantiza el nivel alto de protección exigido por los arts. 81.1 b) y 101 RLOPDCP.

[585] En el mismo sentido la STS 267/2010, de 31 de marzo, la STS 125/2009, de 30 de diciembre y la STS 327/2010, de 12 de abril.

[586] RODRÍGUEZ LAÍNZ, J. L. "De vueltas con SITEL" ob. cit. págs. 4 y 5 "*La confianza en la fiabilidad del sistema es plena, hasta el punto que, llega a desarrollar aparentes presunciones de autenticidad, complitud e inalterabilidad, que tendrán una repercusión directa en el equilibrio de cargas probatorias en sede de enjuiciamiento. El principal peso argumentativo de esa especie de presunción de*

Por su parte, la STS 753/2010, reconoce que dicho sistema "*cumple con todas las exigencias y garantías propias de esta clase de diligencias de investigación y probatorias que cuentan con una previa autorización judicial para su práctica".*

Y para la La STS 705/2010, de 15 de julio, "(...)*cualquier hipotética manipulación dejará rastro de su realización, lo que en principio se evita mediante la fijación horaria, haciendo imposible su manipulación, pues esa constatación horaria evidencia la manipulación que pudiera realizarse*"[587].

En definitiva, lo que resulta indispensable cualquiera que sea el sistema que se utilice es que éste garantice que después de cada conversación, mensaje o chat

---

autenticidad radica en que considera de suma dificultad la manipulación de las grabaciones, como consecuencia de que todo el esquema de seguridad tendente a garantizar la conservación de la información almacenada en el centro de recepción obedece a las exigencias reglamentarias de un nivel alto de seguridad que, por mandato del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento que desarrolla la Ley de Protección de Datos –RLOPDCP-, entre otras cosas, garantiza la inalterabilidad de la información almacenada, así como un efectivo y riguroso control de los accesos que se han producido a aquélla; de hecho, la sentencia asegura que en SITEL este nivel de seguridad existe y está garantizado. Esa apariencia de autenticidad, que no presunción de autenticidad, al no estar amparada en norma de derecho positivo alguno que permita dar fe pública a los soportes físicos en los que se facilita la información interceptada a la autoridad judicial, llevan al Alto Tribunal a establecer una auténtica desviación de las cargas procesales que se hacen residenciar en su esencia en aquel que opone cualquier tacha de autenticidad, manipulabilidad u omisión relevante; y ello no solo por razón de lo que considera es una constatada realidad: la garantía de un nivel alto de seguridad en el funcionamiento de SITEL; sino también por el argumento adicional de que la sola especulación de esa posible manipulación entrañaría imputar la comisión de una grave infracción criminal a los funcionarios públicos encargados de la conservación, acceso y tratamiento de la información canalizada a través del centro de recepción; delito que de ser constatado, dejaría abierta, en su caso, la vía del recurso de revisión. La sentencia es consciente de que esa manipulación es técnicamente posible, pero a su vez destaca cómo el nivel de seguridad alto aplicado al sistema permite un control de accesos que facilitaría seguir el rastro tanto del hecho mismo de la manipulación como de su responsable. Por ello, llega a concluir que: "En todo caso, no es absolutamente descartable una posible manipulación pero su demostración tiene que nacer de datos objetivables e irrefutables". La sentencia comentada considera que, por tanto, no basta con una mera impugnación formal de la prueba, un simple alegato de posibles alteraciones u omisiones, sino que impone que tal alegato se fundamente en una demostración empírica basada en datos objetivos; demostración que solamente podría tener lugar en base a la práctica de una prueba pericial, auditoría informática, que permitirá realizar un juicio de valor sobre la posibilidad, riesgo o realidad de que la manipulación ha podido haberse producido, así como su trascendencia en la garantía de autenticidad de la información facilitada a la autoridad judicial. Dada la complejidad de la prueba requerida para tal menester, se considera que la sede natural para su proposición no habría de superar en ningún caso el umbral del juicio oral, es decir, no más allá de la presentación del escrito de defensa; aunque su sede natural habría de ser la fase de instrucción, una vez que las defensas han sido suficientemente instruidas de la existencia de la interceptación realizada y tenido posibilidad de obtener un cabal conocimiento de su alcance y contenido.

[587] RODRÍGUEZ LAÍNZ, J. L. "De vueltas con SITEL". ob. cit. pág. 6. "*El agente facultado, es obvio, debe acceder al contenido de la información almacenada en SITEL, pero no cuenta con capacidad técnica para alterar la información que allí almacena. Cualquier intento de manipulación o alteración debería pasar por generar archivos falsos o borrar o excluir del soporte CD o DVD conversaciones relevantes; y frente a ello siempre tendríamos el respaldo de acudir al original protegido en la sede de SITEL".*

interceptado por los agentes se proceda al sellado tecnológico del archivo de sonido o imagen con el fin de salvaguardar su integridad, excluyendo cualquier riesgo de manipulación, de tal modo que quede constancia de que la información que se ha facilitado a la autoridad judicial llega a ésta íntegra e inalterada, correspondiéndose fielmente con aquello que se conserva en el centro de recepción.

2.2.D) *Requisitos técnicos para los registros de dispositivos.*

Existe en la LECrim una norma específica para el juicio de fiabilidad aplicable al registro de dispositivos, consistente en que el propio Juez de Instrucción fija los términos y alcance del registro y autoriza la realización de copias de los datos informáticos, fijando también las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación para hacer posible, en su caso, la práctica de un dictamen pericial (art. 588 sexies c).

Algún autor sostiene que la LECrim no contiene medidas eficaces de custodia que permitan esclarecer sin lugar a dudas que dichos dispositivos no han sido alterados desde el momento de su aprehensión hasta la autorización judicial para examinar su contenido, caso de ser esta concedida posteriormente[588].

Quizás hubiera resultado más conveniente que reglamentariamente se establecieran las condiciones o elementos básicos que en el registro de dispositivos

[588] RUBIO ALAMILLO, J. "La informática en la reforma de la Ley de Enjuiciamiento Criminal". ob. cit. pág. 7 "entiende que no se ha dispuesto normativa legal para garantizar la conservación de la cadena de custodia de los dispositivos informáticos intervenidos. Esto significa que se deja, en cada caso particular, a la libre disposición del juez y de los agentes de la Policía Judicial, la forma efectiva en que se llevará a cabo la mencionada conservación de la cadena de custodia; "*No es admisible que la nueva Ley de Enjuiciamiento Criminal nazca coja en esta importantísima parte del proceso teniendo en cuenta, sobre todo, los enormes quebraderos de cabeza que suelen dar las pruebas que aparentemente se detectan como contaminadas o posiblemente contaminadas. Por ejemplo, en un encargo reciente del perito que suscribe, el Cuerpo Nacional de Policía intervino a un acusado una serie de discos duros con vídeos cuyo contenido era ilegal según el art. 189 del Código Penal. Pues bien, tras un examen pormenorizado de los autos, se descubrió que en el inventario de los vídeos realizado por la Policía Judicial en la intervención del domicilio del acusado, acta del secretario judicial, ahora letrado de la administración de justicia, había menos vídeos y algunos de sus títulos eran distintos, que los que detectó la sección de Informática Forense del Cuerpo Nacional de Policía dos años después, cuando analizó los discos duros y redactó su informe pericial"*.

garanticen la fiabilidad del material objeto de investigación y no limitarse solamente a hacer posible un dictamen pericial, sino también, establecer qué condiciones las que garantizan la integridad de los datos objeto de registro[589]. Algún autor habla de protocolización[590].

Si se analiza el precepto citado relativo al juicio de fiabilidad, en el registro de dispositivos informáticos se establece que el Juez "*podrá autorizar la realización de copias de los datos informáticos*". La Ley no especifica la forma en la que se efectuarán estas copias, ni tampoco dice que se realizarán copias de los dispositivos (discos o memorias), sino *de los datos*, lo que significa, que se autoriza la realización del volcado o clonado[591].

En realidad, más que una copia de los datos (copia lógica) lo que resulta necesario realizar es una copia física o clonación (para que también se copien los archivos borrados)[592]. En informática forense se usa el término *clonar*, (que no *copiar*, que es un concepto distinto) para referirse a una tarea de reproducción fidedigna del contenido de los discos duros y demás dispositivos de forma rápida y proporcionar un código *hash* al investigador, calculado a partir de un algoritmo de cifrado estándar[593].

---

[589] Es más que probable que a la hora de autorizar un registro de dispositivos informáticos, el juez no tenga conocimiento de cuáles son esas condiciones que garantizan la integridad y preservación de datos. De ahí la necesidad de una normativa reglamentaria que contemplara las singularidades en este tipo de diligencias y permitiera orientar al juez en la adopción de las mismas.

[590] DELGADO MARTIN, J. "Investigación del entorno virtual (…)". ob. cit. pág.14.

[591]DELGADO MARTIN, J. "Investigación del entorno virtual (…)". ob. cit. pág. 14.

[592] RUBIO ALAMILLO, J. "La informática en la reforma de la Ley de Enjuiciamiento Criminal". ob. cit. pág. 7. "*Normalmente, cuando se copian datos directamente de un dispositivo a otro (en lo que se denomina copia lógica), los archivos borrados no se copian, razón por la cual es necesario ejecutar una copia física o clonación"*.

[593] El procedimiento técnico de clonación de un disco duro. *Vid.* RUBIO ALAMILLO, J. "Clonación de discos duros en el peritaje informático". http://peritoinformaticocolegiado.es/clonacion-de-discos-duros-en-el-peritaje-informatico/ 9/3/2016 a las 20:04 horas.
Se ha de partir de la base de que un disco duro no puede ser nunca clonado mediante herramientas de software.
Cualquier "clonación" mediante herramientas de software no será tal, puesto que el propio proceso de "clonado", teniendo que instalar un software específico para tal fin, alteraría el contenido del disco y lo invalidaría a nivel forense. Asimismo, un "clonado" mediante software que, como se acaba de especificar, no es tal; únicamente suele copiar los ficheros indexados por la instalación actual del sistema operativo, obviando en la copia los sectores ocupados por ficheros procedentes de instalaciones previas y que, obviamente, ya no están en el índice.
El disco duro ha de clonarse, por tanto, usando herramientas de hardware, es decir, mediante lo que se denominan "clonadoras". Existen en el mercado multitud de clonadoras profesionales, que incluso

Para llevar a cabo el clonado de forma correcta, resulta necesario proceder a dos actuaciones: en primer lugar, la realización de una copia espejo o bit a bit de la información original en el mismo lugar en el que encuentra el dispositivo, y se realiza mediante una herramienta de hardware, de tal forma que se lleva a cabo una copia física del contenido del dispositivo; y, en segundo término, la fijación del código hash que se calcula a partir de un algoritmo de cifrado estándar que posibilita concluir que los datos hallados en el dispositivo en el momento de su aprehensión no han sido objeto de ulterior manipulación.

El clonado debe realizarse mediante la utilización de mecanismos que garanticen que no existe contacto con los datos, la mera conexión de un disco duro o memoria USB a un ordenador personal para proceder a su análisis, sin necesidad de interactuar con el disco, contamina la prueba de forma irremediable. Para evitar esta contaminación, es necesario el uso de bloqueadoras de escritura, que son dispositivos que actúan como *puente* entre el disco duro o memoria y el ordenador, de tal forma que el disco o memoria nunca se conectan directamente al ordenador, sino a la bloqueadora, siendo ésta la que se conecta finalmente a la máquina[594]. En cualquier caso, los agentes que realicen el volcado de los datos, deberán dejar constancia documental de cuál ha sido el mecanismo utilizado para su incorporación al proceso. Esta documentación es lo importante en el juicio de fiabilidad pues permite comprobar el modo en el que se ha efectuado la clonación sin que exista tacha alguna, por lo que sería relevante la homologación de equipos y programas.

---

permiten copiar varios discos a la vez y/o realizar varias copias de un mismo disco. El clonado hardware copia, bit a bit, el contenido del disco origen en el disco destino, que debe ser de igual o superior capacidad que el disco origen. Así pues, una vez se tienen el original y un disco destino virgen de igual o mayor capacidad, se deben colocar en la clonadora, cada uno en su slot correspondiente (teniendo mucha precaución en no equivocarse de slot ya que un error sería absolutamente fatal), y se procede con la clonación. Como se trata de una copia física (a nivel de bit), es bastante probable que, si el disco duro origen es grande y la clonadora no es muy rápida, el proceso se demore durante varias horas. Finalizado el proceso, la clonadora confirmará que los discos son idénticos bit a bit (de lo cual dará fe el fedatario público) y se tendrán dos discos duros con exactamente el mismo contenido; el original y el clonado. Cualquier clonadora tiene la funcionalidad de comprobar, en cualquier momento, si dos discos cualesquiera son idénticos, sin necesidad de que la copia haya tenido que realizarse de forma inmediatamente anterior. Las clonadoras comprueban que los discos son idénticos bien comprobando bit a bit, bien calculando el valor de un determinado *algoritmo de hash*.

[594] RUBIO ALAMILLO, J. "La informática en la reforma de la Ley de Enjuiciamiento Criminal". ob. cit. pág. 7.

El clonado de la información determinará la existencia de lo que podríamos llamar un "original" y una "copia" (clonado)[595], en la que el perito llevará a cabo las actuaciones para elaborar el informe; y eventualmente una "copia 2.a", que habría de permanecer en poder de la persona o empresa que ostente la titularidad de los datos, para que ésta pueda continuar sus actividades.

En definitiva, el clonado garantiza que "original" y "copia" son exactamente iguales, para lo cual es necesario utilizar dos tipos de garantías:

- **Garantías técnicas**, relativas a la utilización de instrumentos tecnológicos y procedimientos adecuados que deberán indicar en el informe anexo o atestado cómo se ha realizado dicho proceso. Dependerá del material que se tenga que clonar[596]. Lo importante, sea cual sea el método usado es que se deje constancia del hash.

[595]RUBIO ALAMILLO, J. "Clonación de discos duros en el peritaje informático". http://peritoinformaticocolegiado.es/clonacion-de-discos-duros-en-el-peritaje-informatico/ 9/3/2016 a las 20:04 horas.
"El perito informático deberá tener en cuenta que el disco clonado ahora es "su" disco original y que, por tanto, no podrá trabajar sobre el mismo, teniendo que realizar un clonado privado del mencionado disco con una clonadora de su propiedad, tal y como se advirtió al principio del artículo. Esto es una medida de seguridad que el perito informático debe tomar para evitar sorpresas a la hora de manipular el disco ya que, aunque el notario o el secretario judicial tienen copias que se pueden volver a clonar, los honorarios de un notario son elevados y el tiempo de un secretario judicial escaso, además de no quedar muy profesional el tener que realizar una nueva copia por un descuido.el secretario judicial garantizará la operación con su supervisión jurídica que, una vez finalizada, cerrará con el precinto del disco duro original, que quedará bajo su poder de custodia, para posibles futuros contrastes y/o contraperitajes, cediendo la copia clonada a los peritos para que, sobre ella, practiquen los oportunos análisis y pericias, sin riesgo de borrar o alterar la fuente original de prueba. Por lo tanto, el clonado o volcado del disco duro no es sino una operación".

[596] Si se trata de discos duros de poca capacidad se suele usar una clonadora tipo Hard Copy III, que el proceso de clonado es aproximadamente una hora y treinta minutos para clonar un disco duro de 250 megas y obtener el hash. A ello hay que sumar el tiempo invertido en wipear (borrar el restante) el disco duro clonado en la parte que no se ha clonado. A modo de ejemplo si se han clonado 250 megas y el disco duro en el que se copia tiene una capacidad de 750 megas, los 500 megas restantes que no se han usado serán wipeados. Finalmente, obtenemos el hash de la copia clónica que es exactamente igual que el del disco duro original.
En el que caso de que se tenga que clonar discos duros de gran capacidad o muchos de ellos, como el proceso con las clonadoras es bastante lento, se suele recurrir al apoyo de equipos con distintos puertos y se bloquea el puerto contra escritura y se extrae el contenido con los programas *FTK* y *guy manager, LINUS*, se podrán extaer los archivos borrados si no se han sobreescrito. Si se han de clonar un pen drive, se hace de la misma forma bloqueando el puerto contra escritura.
En el caso de que se haya de clonar un móvil. Existe un programa denominado *UFED celebrite*, donde se analiza y se presentan todos los archivos en formato PDF o HTML con sus enlaces.
Otra opción al clonado, es hacer una imagen física de lo que se pretende clonar. Programas como guyen manager o FTK montan la Unidad de disco. Y el programa autopsi, analiza todo el material, y se genera el informe.

- **Garantías jurídicas**, es decir, presencia de testigos y/o fedatario público (Notario o LAJ) siendo preferible la segunda opción por los propios efectos de la fe pública[597]. En la práctica la duración del clonado hace que el material objeto de registro se desplace a la oficina judicial y sea allí donde se proceda al clonado.

Ahora bien, el Tribunal Supremo ha relativizado la obligatoria presencia del LAJ resolviendo que "*ninguna garantía podría añadirse con la presencia del Secretario Judicial al que no se le puede exigir que permanezca inmovilizado durante la extracción y ordenación de los datos, identificando su origen y procedencia".* (STS 1599/1999 de 15 de noviembre [FJ 2º. Ap.3]. Comparto la opinión de que no es necesario que esté presente en todo el proceso, eminentemente técnico, bastando con que esté al inicio y al final. Para garantizar que coincide lo ocupado y la copia se hace la prueba técnica de contraste o hash, antes y después del análisis, de forma que cualquier modificación del contenido del soporte durante el análisis arrojaría un hash distinto, por lo que si coinciden queda demostrada su integridad, no siendo necesario que esté presente durante el desarrollo del volcado[598]. En definitiva, existen medios tecnológicos que permiten que se garantice la autenticidad e integridad de la fuente de prueba.

El volcado ante el LAJ resulta conveniente para garantizar la preservación de la información, pero no es requisito de validez de la prueba de tal manera que su ausencia no determina su nulidad. El practicado sin su presencia no es una prueba preconstituida, sino que ha de llevarse al juicio oral por otras vías, especialmente mediante la declaración de los agentes que realizaron el volcado que será valorada por el tribunal de enjuiciamiento[599].

Siguiendo con el análisis del artículo (art. 588 sexies c LECrim), la segunda parte es clave para el juicio de fiabilidad, pues dispone que el juez fijará "*las*

[597] DELGADO MARTIN, J. "Investigación del entorno virtual (…)" ob. cit. pág. 15.

[598] Existen varias sentencias del Tribunal Supremo (SSTS 1599/1999 de 15 de noviembre, 256/2008 de 14 de mayo y 480/2009 de 22 de mayo) que no la consideran necesaria porque "*ninguna garantía podría añadirse con la presencia del Secretario judicial al que no se le puede exigir que permanezca inmovilizado durante la extracción y ordenación de los datos, identificando su origen y procedencia".*

[599] Así se desprende de la STS 256/2008 de 14 de mayo de 2008 que no acordó la nulidad de dicha prueba practicada sin la presencia del LAJ, sino por los técnicos policiales en su sede, porque la "*presencia del Secretario habría sido de facto tan inútil e innecesaria como la que pudiera darse en el desarrollo de cualquier otra de las muchas imaginables en cuya técnica el fedatario judicial no fuera experto".*

condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación".

En ningún caso se indica en el artículo *cómo* se debe producir el acceso a la información al objeto de garantizar la integridad y las garantías de preservación de los datos informáticos, sino que será el Juez quien lo determine. Y he aquí un punto fundamental, y cuya falta genera consecuencias muy graves para el juicio de fiabilidad, pues no puede obviarse que un disco duro o memoria es un dispositivo que puede ser fácilmente manipulado que incluso puede no dejar rastro de la manipulación[600]. De ahí que las garantías del acusado quedarían a merced de la fijación de esas condiciones[601].

[600]RUBIO ALAMILLO, J. "La informática en la reforma de la Ley de Enjuiciamiento Criminal". ob. cit. pág. 8. "*los dispositivos, programas y bases de datos informáticas son manipulables sin que muchas veces pueda detectarse tal manipulación, ni siquiera por peritos informáticos"*

[601]Alguien malintencionado podría desprecintar cuidadosamente el disco duro, manipularlo sin dejar rastro y volver a colocar el precinto. Cualquier suspicacia sería evitada con una clonación in situ del material intervenido, delante del LAJ y a ser posible del investigado y su letrado, obteniendo los códigos *hash* correspondientes para cada disco duro y su copia clónica.
Es importante en la práctica de volcado destacar la STS 342/2013, de 17 de abril [FJ 8º]. La defensa primero pone el acento en el hecho de que el acta en el que fue recogida la diligencia de volcado no aparecía debidamente firmada por la Secretaria. Se responde por la Sala que "*es cierto que se trata de una irregularidad formal que debió haber sido subsanada. Pero no olvidemos que no estamos en presencia de un documento ajeno al proceso que se incorpora al mismo para su valoración probatoria. Se trata de un documento judicial, unido formalmente a la causa, que describe la presencia de los dos agentes de policía en las dependencias judiciales para la práctica de un acto de volcado que había sido previamente autorizado por el Juez. Dudar de la integridad de ese documento por la falta de firma del Secretario ante el que se practica la diligencia carecería de sentido. Pero aun en el caso en que se pretendiera extraer de esa falta de firma algún efecto en orden a la validez del acto, conviene recordar que la jurisprudencia de esta Sala no ha considerado que la práctica de las operaciones técnicas de volcado exija como presupuesto de validez la intervención del Secretario judicial pues ninguna garantía podría añadirse con la presencia del funcionario judicial al que no se le puede exigir que permanezca inmovilizado durante la extracción y ordenación de los datos, identificando su origen y procedencia. la presencia del fedatario judicial en el acto del volcado de datos no actúa como presupuesto de validez de su práctica. Lo decisivo es que, ya sea mediante la intervención de aquél durante el desarrollo de la diligencia de entrada y aprehensión de los ordenadores, ya mediante cualquier otro medio de prueba, queden descartadas las dudas sobre la integridad de los datos y sobre la correlación entre la información aprehendida en el acto de intervención y la que se obtiene mediante el volcado*.
También reprocha la ausencia del interesado y su Letrado en el acto del volcado, así como la falta de expresión de los instrumentos técnicos empleados por los agentes para hacer realidad ese volcado. Sostiene la Sala que ninguna de estas objeciones tiene alcance constitucional pues "*el acusado no estaba detenido, ni en el momento del registro que permitió la intervención de los ordenadores, ni cuando se verificó el volcado. La posibilidad de designar a un perito que esté presente en ese acto (art. 476 de la LECrim) forma parte de las facultades que le asisten en su calidad de imputado. Sin embargo, esa presencia no es presupuesto de validez del acto. Nada de ello se desprende de la literalidad de aquel precepto. Y, lo que es más importante, el acusado contaba con la posibilidad - formalmente ejercida en el plenario- de proponer su propio perito para cuestionar todos aquellos aspectos del volcado que considerara oportuno. Forma parte ya de la valoración probatoria atribuir al dictamen pericial elaborado por los agentes a partir del volcado, la virtualidad incriminatoria que la Audiencia le ha adjudicado. "Lo propio puede decirse respecto de la falta de mención de la metodología técnica que presidió el volcado. No se trató, en modo alguno, de un volcado clandestino. Se verificó en dependencias judiciales, en presencia de la Secretaria judicial y pudo ser contradicho en el plenario mediante el*

En definitiva, el clonado o volcado de datos de los dispositivos es una garantía inicial en el juicio de fiabilidad del registro, pues acredita que lo que se copia es imagen fiel y exacta de lo que se ocupa, y se vincula a la obtención íntegra de la fuente de prueba; integridad vinculada en estas pericias informáticas especialmente al hecho de la modificabilidad y volatilidad mayor que en otras, por sus características, que va a servir objetivamente para garantizar la corrección de la información sobre la que va a versar después la pericia, y subjetivamente, para garantizar una defensa justa.

La finalidad de esta operación es, por un lado, preservar la fuente original de prueba intacta e inmodificada conforme sale del ordenador del investigado, razón por la que suele precintarse quedando en poder del custodio de las pruebas judiciales, a disposición de las partes y de la causa, y por otro, permitir con la copia trabajar a los peritos informáticos sobre un elemento igual a la evidencia ocupada, pero sin el riesgo de una alteración culposa o dolosa de su contenido, que lleve a conclusiones erróneas.

Por tanto, la identificación y precinto de los ordenadores intervenidos y de sus puertos (STC 170/2003, de 29 de septiembre) es otra garantía en el juicio de fiabilidad. Y aunque la LECrim no diga nada al respecto también será importante que el LAJ y los agentes policiales comisionados por el juez no olviden consignar en el registro de dispositivos cuantos datos permitan identificar al presumible usuario del ordenador donde se ocupen los efectos delictivos, archivos y documentos objeto de la investigación, aprehensión de las claves de usuario y contraseñas que se descubran, apodos o *nicks* que se encuentren junto al ordenador y que no se escatime en datos técnicos (como serían, por ejemplo, en los supuestos de pornografía infantil, la indicación del número y nombre de los archivos, el número de fotografías e imágenes encontrados, su impresión en soporte duradero y los megas de su capacidad y ocupación, etc). Todo ello será crucial para asegurar la fiabilidad del material probatorio.

En caso de que se intervengan los equipos o el material informático por la Policía, hasta que se entreguen al fedetario judicial (o al perito para su examen), debe garantizarse que lo entregado sea exactamente lo ocupado.

---

interrogatorio de los agentes de policía que lo verificaron y con el dictamen del perito aportado por la propia defensa".

Deben examinarse los momentos de recogida, custodia y examen de las piezas de convicción o cuerpo u objeto del delito[602]. Lo hallado deber ser descrito, tomado, puesto en depósito y analizado con las debidas garantías. El art. 338 LECrim, previene que los instrumentos y efectos del delito se recogerán de tal forma que se garantice su integridad, y el Juez acordará su retención, conservación o envío al organismo adecuado para su depósito[603].

Para ello, como recuerda la STC 170/2003, de 29 de septiembre de 2003, en interpretación del art. 338 LECrim, se deben cumplir una serie de requisitos[604]:

1. La descripción del material ocupado en acta o diligencia del LAJ (art. 334 LECrim) y en su presencia debe procederse igualmente al bloqueo y precinto de cualquier ranura o puerto.

2. Custodia en un lugar adecuado (para evitar su deterioro o manipulación).

[602] RUBIO ALAMILLO, J. "La dirección IP en el peritaje informático". Abril de 2015. http://peritoinformaticocolegiado.es/la-direccion-ip-en-el-peritaje-informatico/. 18/2/2016 a las 20.19 horas.
Una vez los discos duros han sido clonados, es necesario analizar las copias obtenidas. El análisis de los discos duros debe focalizarse sobre los *ficheros de log* de los sistemas atacados o mediante los que se ha cometido el delito. Un *fichero de log* es un archivo informático que registra todas las actividades de un sistema informático. Así pues, es necesario que los *ficheros de log* sean analizados concienzudamente al objeto de poder determinar el momento exacto de comisión del delito y la dirección IP desde la que se realizó dicha actividad delictiva. Una vez se haya obtenido la dirección IP desde la cual se ha cometido el delito, así como la fecha y hora de comisión, dichos datos deberán ser cotejados con el operador, al objeto de conocer quién es el abonado que estaba tras la dirección IP en el momento en el que se cometió el delito. Es necesario también tener en cuenta ciertas variables importantes, como que por ejemplo, la fecha y la hora del sistema informático que está siendo analizado, puede no coincidir con la fecha y la hora de los sistemas informáticos del operador, o pudo no coincidir en el momento en el que se estaba cometiendo el delito

[603] *Artículo 338 de la LECrim*
"Sin perjuicio de lo establecido en el Capítulo II bis del presente título, los instrumentos, armas y efectos a que se refiere el artículo 334 se recogerán de tal forma que se garantice su integridad y el Juez acordará su retención, conservación o envío al organismo adecuado para su depósito".

[604] Fundamento jurídico III. "(…)los soportes informáticos no solo no fueron identificados para determinar el domicilio en el que fueron intervenidos, sino que tampoco se procedió a su correcto sellado y precintando. A ello debe unirse el hecho objetivo de la existencia de una significativa discordancia numérica entre los CD-ROM intervenidos. Ello acredita que se ha producido una deficiente custodia policial y control judicial de dicho material, que no estaba debidamente precintado y a salvo de eventuales manipulaciones externas tanto de carácter cuantitativo (número de las piezas de convicción halladas en los registros) como cualitativo (contenido de aquellos soportes que admitieran una manipulación por su carácter regrabable o simplemente por su naturaleza virgen en el momento de su incautación, e incluso su sustitución por otros), lo que impide que pueda afirmarse que la incorporación al proceso penal de los soportes informáticos se diera con el cumplimiento de las exigencias necesarias para garantizar una identidad plena e integridad en su contenido con lo intervenido y, consecuentemente, que los resultados de las pruebas periciales se realizaran sobre los mismos soportes intervenidos o que éstos. no hubieran podido ser manipulados en cuanto a su contenido.

3. Control judicial de la recogida y custodia. La carencia de dicho control afecta a la validez de la prueba, por vulneración del derecho a un proceso con todas las garantías[605].

Y todo ello, como recuerda la STS 1045/2011, de 14 de octubre para garantizar que desde que se recogen los vestigios relacionados con el delito hasta que llegan a concretarse como pruebas en el momento del juicio, aquello sobre lo que recaerá la inmediación, publicidad y contradicción de las partes y el juicio del tribunal es lo mismo. Es decir, es necesario tener la seguridad de que lo que se traslada, analiza o, en este caso, se visiona, es lo mismo en todo momento, desde que se interviene hasta el momento final que se estudia y analiza[606].

No han de surgir especiales problemas cuando se trata de la incorporación al proceso del propio dispositivo electrónico, ya sea por quedar bajo la custodia del LAJ o por quedar en posesión de la Policía Judicial u organismo especializado a disposición del Juez.

De otro lado, es muy frecuente en los delitos de injurias, amenazas, acoso, contra la intimidad etc., que la víctima acuda a la Policía o al Juzgado con el terminal o dispositivo que lo contiene, el cual podrá recogerse como cuerpo del delito, pero en la mayoría de las ocasiones lo que se hace es una transcripción o transmisión a papel del mensaje a fin de incorporarlo al proceso. El LAJ debe realizar un cotejo de las transcripciones con el texto original y tal diligencia constituirá una prueba documental que se valorará como tal junto al resto de la prueba que se practique en el juicio sobre ella (declaraciones del acusado, testigos y sobretodo la pericial efectuada en ese material según la STS 300/2015). Igualmente, sucede con la aportación por parte de la víctima del correo electrónico recibido.

---

[605]STC 170/2003, de 29 de septiembre de 2003, Fundamento Jurídico 3 in fine. *"(...)en la medida en que se han valorado como actividad probatoria de cargo los informes periciales efectuados sobre un material informático que se incorporó sin que quedara acreditado el cumplimiento de las debidas garantías de custodia policial y control judicial sobre su identidad e integridad, debe declararse que se ha vulnerado el derecho a un proceso con todas las garantías".*

[606] FIGUEROA NAVARRO, C Y DEL AMO RODRÍGUEZ, A. "La cadena de custodia de las pruebas y los protocolos de actuación de la policía científica". Policía Científica. 100 años de ciencia al servicio de la Justicia. Ministerio del Interior. Material de las Jornadas Centenario de la Policía Científica Española, junio 2011.

En definitiva, del volcado a papel en un registro se levantará un acta o diligencia, en la que se reflejará las personas intervinientes, se describirá lo que se ha hecho y se firmará por todos los intervinientes.

2.2.E) *Requisitos técnicos para el registro remoto.*

Especial importancia plantea el juicio de fiabilidad en este tipo de registro, al ser la diligencia de investigación más invasiva, pues permite que el juez pueda autorizar la utilización de datos de identificación y códigos o la instalación de un software, para de forma remota y telemática, proceder al examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos. La propia resolución judicial que autorice la medida deberá responder pormenorizadamente a todos sus extremos, desde qué dispositivos se van a controlar, hasta los agentes encargados de llevar dicha medida a cabo.

La resolución judicial habilitante de la medida deberá contener una serie de menciones ya examinadas anteriormente (*vid.* art. 588 septies a, apartado 2º LECrim). Todas esas menciones deberán constar expresamente para asegurar la fiabilidad del material objeto de registro, así tendrá que identificarse sin equívocos:

1. Qué ordenadores, dispositivos electrónicos o sistemas informáticos o parte de los mismos, medios informáticos de almacenamiento de datos o bases de datos, datos u otros contenidos digitales han sido objeto de esta medida.

2. Cómo se ha procedido al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el software utilizado.

La primera modalidad contemplada por el precepto radica en la "*utilización de datos de identificación y códigos",* es decir, se trata de aquellos casos en los que los investigadores acceden a distancia al contenido del dispositivo mediante el uso de

códigos u otros elementos identificativos pero sin la instalación en el mismo de software alguno.

La segunda modalidad consiste en "*la instalación de un software*". Son aquellos supuestos en los que se accede al contenido de un dispositivo electrónico mediante la previa instalación en el sistema investigado de un software (de los denominados programas troyanos) que permite a las autoridades escanear un disco duro y demás unidades de almacenamiento y remitir de forma remota y automatizada el contenido del mismo al informático de la autoridad responsable de la investigación[607].

Lo importante, será que se determine qué tipo de programas informáticos "espía" se ha utilizado en el curso del registro remoto, para saber las posibilidades que ofrece y los límites en las acciones que pueden realizar dichos programas, así como la posibilidad de verificar que efectivamente no se han extralimitado en sus funciones[608].

3. También es una garantía en el juicio de fiabilidad saber qué agentes han sido los encargados de practicar este registro remoto, a efectos de su identificación y de una posible contradicción en juicio como testigos acerca de todo el proceso seguido.

4. Respecto a la posibilidad de realizar copias de los datos así como su conservación, debe hacerse una remisión a lo dicho sobre las copias en el registro de dispositivos que será plenamente aplicable. La volubilidad del soporte (más tangible y alterable que el del papel) obliga a modos novedosos de conservación de la información y datos observados que a su vez determinan diferentes formas de conocerlos y

[607] Téngase en cuenta que los troyanos constituyen la única forma de efectuar un *bypass* a los ISP, lo que posibilita investigaciones en las que no se dependa de instituciones privadas para resolver un delito, ya que el troyano puede interceptar la conexión misma sin necesidad de requerir un auxilio técnico de los ISP. Aunque un problema con el que se enfrentarán este tipo de software, es que en realidad al tratarse de virus que se introducen en el ordenador del investigado, hay que neutralizar el antivirus de éste para que puedan operar.
También cabría plantear la inclusión de los *keylogger*, que son instrumentos que almacenan cada una de las pulsaciones que se hagan en el teclado de un ordenador. Pueden ser hardware, esto es, adaptadores que se conectan en dicho ordenador o en su teclado; o bien software, es decir, programas que se instalan en el ordenador investigado ejecutables sin que el usuario se dé cuenta, que guardan cada tecla presionada en el teclado, y cuya información puede ser transmitida al investigador por una red local o de telecomunicación.

[608] RUBIO ALAMILLO, J. "La informática en la reforma de la Ley de Enjuiciamiento Criminal". ob. cit pág. 9 "*sería conveniente establecer los programas informáticos que se utilizarán como troyanos para espiar a los sospechosos, para saber el alcance de los mismos y almacenarlo en bases de datos seguras, junto a sus códigos hash para evitar cualquier posible manipulación malintencionada sobre los mismos".*

reproducirlos que, jurídicamente, obligan a extremar las garantías de integridad e inmodificabilidad de lo duplicado[609].

Una vez más, no se establecen qué medidas van a ser las que preservarán la integridad de los datos garantizando la autenticidad de la información. Lo tendrá que decidir el juez. A diferencia del registro de dispositivos donde el LAJ al menos está presente en el escenario del registro, levantando acta y dando fe de lo incautado, no sucede lo mismo en el registro remoto, donde los encargados de efectuarlo son los agentes designados y sin que esté presente obviamente el LAJ en la práctica del mismo. Por ello, debiera articularse un sistema en el que exista plena garantía de que lo que se está registrando remotamente es cierto y veraz hasta su concreción como pruebas en el momento del juicio.

2.2.F) *La fiabilidad del agente encubierto informático.*

Respecto a la información obtenida por el agente encubierto informático, es necesario determinar con exactitud por un lado el canal cerrado de comunicación al que se ha accedido y la forma de acceso al mismo además del tipo de archivo ilícito que se pretende intercambiar o enviar, el destino de esos archivos y el control que pueda establecerse sobre el movimiento de los mismos en la red tanto en orden a la posibilidad de su posterior recuperación y también para evitar el riesgo de provocación delictiva.

En la práctica, las posibilidades que ofrecen el uso de este tipo de archivos son muy amplias, inclusive el envío y recepción de archivos ilícitos a través de una *backdoor* sin que el sospechoso se percate, de tal forma que luego podrían ser utilizados judicialmente en su contra[610].

---

[609] VELASCO NÚÑEZ, E. "Novedades técnicas de investigación penal vinculadas a las nuevas tecnologías", Revista de Jurisprudencia el derecho nº 4, febrero de 2011. pág. 6.

[610] RUBIO ALAMILLO, J. "La informática en la reforma de la Ley de Enjuiciamiento Criminal". ob. cit. pág. 3. *Dichos archivos ilícitos, incluso, podrían aparecer en inventarios o en informes periciales policiales posteriores como material ilícito hallado en nuestros discos duros o memorias, debido a que, si no existe un inventario efectivo de dichos ficheros ilícitos que vayan a ser utilizados como señuelo,*

El *hash* es pieza clave para el juicio de fiabilidad del material probatorio, el poder controlar los archivos ilícitos intercambiados. Ahora bien, se precisa la existencia de un registro pormenorizado de los ficheros que vayan a ser utilizados como *señuelos* por parte de la Policía, que estén auditados y almacenados en bases de datos seguras, junto a sus códigos *hash* para evitar cualquier posible manipulación malintencionada sobre los mismos, pues sin ese control ningún proceso judicial tendrá las debidas garantías procesales[611].

2.2. G) *Consecuencias de la falta de fiabilidad.*

El juicio de fiabilidad de las pruebas informáticas es de suma importancia pues da transparencia a la actuación practicada por la Policía, permite comprobar cómo se ha obtenido determinada información, cuál ha sido el medio técnico usado para ello, el procedimiento utilizado en su obtención, cómo se ha practicado una determinada diligencia, controla la veracidad de lo suministrado para el caso de plantearse alguna discusión al respecto poder practicar la correspondiente prueba pericial y en definitiva, permite comprobar si se han adoptado las medidas precisas de seguridad que garantizan la integridad, autenticidad, confidencialidad, calidad, protección y conservación de la información obtenida.

En eso consiste el juicio de fiabilidad: en comprobar que se han cumplido todas las prescripciones técnicas en la adopción de la medida y que el material aportado en

auditados por profesionales externos y almacenados, cada uno de ellos, en una base de datos segura junto a su correspondiente código hash para evitar su manipulación, no sería posible distinguirlos del material ilícito realmente obtenido por el acusado sin la ayuda policial. Además, es necesario incidir también en el hecho indiscutible que supone como incitación a cometer una actividad delictiva el envío de un fichero ilícito a un ciudadano, toda vez que, un delincuente real, podría diseminar estos archivos por la red sin control, siendo encontrados en intervenciones domiciliarias por la Policía Judicial y sin saber si realmente dichos ficheros fueron enviados por la Policía como señuelo, o por delincuentes reales que tomaron esos ficheros policiales y luego los diseminaron como parte de su actividad criminal.

[611] RUBIO ALAMILLO, J. "La informática en la reforma de la Ley de Enjuiciamiento Criminal". ob. cit. pág. 9 Sin un registro, de ficheros *señuelo* y *troyanos*, sería virtualmente imposible discriminar qué archivos han sido enviados por los agentes encubiertos o por *troyanos*, en lugar de ser conseguidos de forma ilícita por el sospechoso, por lo que se podría dar la paradoja de que un ciudadano fuese condenado por tener en su posesión y, eventualmente, distribuir, archivos ilícitos que en realidad le fueron enviados como *señuelos* por parte de algún agente encubierto de la Policía o de algún *troyano* policial.

juicio es el mismo que en su día se recogió sin tacha alguna en la investigación del delito.

Si se pretende restar eficacia probatoria, habrá que alegar la causa que motiva la falta de fiabilidad del material probatorio, como puede ser:

- La no concreción del "artificio técnico" utilizado para acceder a los códigos tipo IMSI, IMEI de identificación del aparato de telecomunicaciones o a la obtención del número de teléfono o identificación del titular.
- La cesión de datos por parte de las operadoras cuando haya sospechas de que existen irregularidades en las medidas de seguridad implementadas para la conservación de esos datos entre las que se encontrarían: la falta de responsable del fichero, de control en el acceso de dichos datos, resultado defectuoso en la auditoría sobre las medidas de seguridad aplicadas y su cumplimiento que se practica cada dos años, etc...
- La entrega de la intervención de las comunicaciones en soportes digitales sin contar con medidas de seguridad que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados.
- Que los soportes entregados a la autoridad judicial no cuenten con la garantía de sistema de sellado o de firma electrónica avanzada o de sistema de adveración suficientemente fiable.
- Que no estén indicados la identificación de los terminales que contactan entre sí o el origen y destino de cada una de las conversaciones grabadas.
- El sistema en el que se intervienen las comunicaciones no garantice que después de cada conversación, mensaje o chat interceptado por los agentes se proceda al sellado tecnológico del archivo de sonido o imagen con el fin de salvaguardar su integridad.
- Qué exista una posible manipulación del material.
- Si se comprueba que no se procedió al correcto sellado y precintado de los elementos probatorios.

- Si se acredita que se ha producido una deficiente custodia policial de dicho material, que no estaba a salvo de eventuales manipulaciones externas, tanto de carácter cuantitativo como cualitativo[612].

- Que el clonado de los datos se practique con instrumentos tecnológicos o procedimientos no adecuados, que no se indique cómo se ha realizado dicho proceso o que no coincidan los hash del original y copia.

- Qué no conste qué ordenadores, dispositivos electrónicos o sistemas informáticos etc. son objeto del registro remoto. Ni tampoco, cómo se ha procedido al acceso y aprehensión de los datos o archivos informáticos o el software utilizado, ni los agentes encargados de practicar este registro remoto.

- Qué el archivo ilícito empleado por el agente encubierto informático no esté perfectamente identificado.

- Y en general, que se constate la ausencia de control judicial[613] en las medidas adoptadas o que los informes periciales fueron efectuados sobre un material informático que se incorporó sin que quedara acreditado el cumplimiento de las debidas garantías de custodia policial y control judicial sobre su identidad e integridad[614].

Y aún en estos casos dependerá de cual es la causa alegada para restar la fuerza o eficacia probatoria por falta de fiabilidad, pues no es lo mismo alegar la falta de fiabilidad del material por no tener conocimiento de cómo la policía obtuvo el número de teléfono, o porque no se indique cuál ha sido el medio técnico usado para hacer el clonado de datos (STS 342/2013), a que se alegue que los soportes informáticos no

[612] FIGUEROA NAVARRO, C Y DEL AMO RODRÍGUEZ, A. "La cadena de custodia de las pruebas y los protocolos de actuación de la policía científica". Policía Científica. 100 años de ciencia al servicio de la Justicia. Ministerio del Interior. Material de las Jornadas Centenario de la Policía Científica Española, junio 2011.

[613] STC 121/1998, de 15 de junio [FJ 3], STC 49/1999, de 5 de abril [FJ 11].

[614] En relación a la falta de fiabilidad por defectos en la recogida de los elementos informáticos ver STS 714/2016, de 26 de septiembre, STS 587/2014, de 18 de julio, STS 53/2011, de 10 de febrero, SSTS 266/2010, de 31 de marzo, 240/2010, de 24 de marzo 93/2010, de 8 de febrero. ATS 1051/2010, de 27 de mayo. SSTS 221/2009, de 6 de marzo, 1190/2009, de 3 de diciembre, 1349/2009, de 29 de diciembre. STS 501/2005, de 19 de abril. SAP de Málaga (sección 7ª) 19/2013 de 21 de marzo, (cadena de custodia de un Iphone). SAP de Murcia (sección 3ª) 85/2011 de 25 de octubre (cadena de custodia de un disco duro).

estaban identificados, sellados o precintados (STC 170/2003)[615] o que se efectuó un registro de dispositivos sin antes efectuar un clonado.

Alegar la simple posibilidad de manipulación del material objeto de prueba para entender que el material probatorio no es fiable, no parecería aceptable, ya que debería exigirse la prueba de su manipulación efectiva[616]. En definitiva, si se afirma que no existe fiabilidad en el material probatorio, pero se omite explicar las razones por las que se estima que eso ha ocurrido sin concretar la causa de una infracción que directamente se alega sin mayores determinaciones, tampoco será posible apreciar la vulneración de un proceso con todas las garantías por falta de fiabilidad del material probatorio.

3. LA PRUEBA PERICIAL INFORMÁTICA.

La intervención de los peritos informáticos es también una garantía en el juicio de fiabilidad. Lo normal será que el Juzgado haya dictado un auto ordenando realizar la pericia informática al Organismo oficial especializado (Grupo de Delitos Telemáticos de la Guardia Civil (GDT), Brigada de Investigación Tecnológica de la Policía Nacional o los departamentos especializados de la Policía Autonómica (Ertzaintza, Mossos D'Esquadra). También se puede nombrar como peritos a expertos (Ingenieros en Informática o Técnicos en Informática) para que auxilien a la comisión judicial en las entradas y registro y acompañen a la Policía como Peritos Judiciales, lo que puede ser conveniente en la investigación de determinados delitos (ej. propiedad intelectual)[617].

[615] ATS 1647/2014, de 16 de octubre. [FJ 2º] "*Las pruebas practicadas (documentales y testificales) pusieron de manifiesto que, desde la entrada y registro en el domicilio del acusado, el material informático incautado fue trasladado a varias comisarias sin que conste su recepción y debida custodia, y que cuando llegó al Juzgado la bolsa en que se alojaba aquel material estaba desprecintada. Por ello concluye la Sala, razonada y razonablemente, que el material incautado no ha sido objeto de la debida custodia y no puede darse validez al informe pericial".* [FJ 3º] "*(...) En el caso aunque se admitiera la ruptura de la cadena de custodia no existe duda alguna de la autenticidad de las fotografías y de que fueron realizadas por el recurrente, lo que viene a confirmarse por las testificales de los agentes y por el propio reconocimiento del acusado."*

[616] STS 629/2011 de 23 de junio y STS 776/2001, de 20 de julio.

[617] SAP Barcelona, (Sección 7ª) 95/2008 de 29 de enero. En este supuesto, investigándose un presunto delito contra la propiedad intelectual al haberse denunciado el ofrecimiento en una página web de una

Se ha planteado entre la doctrina y la jurisprudencia las cuestiones relativas a la eficacia procesal y a la validez de la prueba pericial (informática, en este caso) practicada directamente por la policía judicial, sin existencia de un mandato judicial expreso que ordene al correspondiente laboratorio oficial o gabinete técnico de la Policía Científica la confección de la pericia. La cuestión ha quedado resuelta en base a que "*la intervención del juez, salvo en supuestos de afectación de derechos fundamentales, no debe impedir la posibilidad de actuación de la policía, en el ámbito de la investigación y averiguación de los delitos en los que posee espacios de actuación autónoma*"[618]. En este sentido, bajo el marco general de habilitación consagrado en los

serie de cracks (herramientas informáticas para anular, burlar o alterar los mecanismos de protección creados específicamente para determinados programas informáticos), el auto autorizando la entrada y registro en la sede de la empresa que alberga el dominio de internet donde se encuentra alojada la referida página web encomienda en su parte dispositiva la práctica de la diligencia a los miembros de la policía judicial encargados de la investigación, para añadir a continuación que la diligencia se practicará con la intervención de los peritos Sres. "...", nombrados para auxiliar a la comisión judicial en la determinación de los efectos que tengan relación directa con los hechos objeto de instrucción, objetos que serán intervenidos y objetos de depósito. Argumenta la Sentencia que tales peritos "*son peritos judiciales nombrados por el Juez de Instrucción* que optó entre una de las tres posibilidades dadas por la denunciante (lista de peritos judiciales, Asociación de Doctores, Licenciados e Ingenieros en Informática (ALI) o Asociación de Técnicos en Informática (ATI)); pues bien el Juez elige esta última y dentro de dicha Asociación se escoge a los finalmente designados. Son peritos por tanto judiciales, no de parte, con obligación de veracidad y sometimiento exclusivo a las reglas de su ciencia, en este caso la informática, y con la consiguiente responsabilidad penal y/o civil para el caso de incumplimiento. Y además como es de ver en la parte dispositiva del auto trascrito el Juez de Instrucción les colocó en una posición de igualdad con la policía a la hora de practicar el registro siendo ellos mismos los que determinarían que efectos debían ser intervenidos y custodiados y por tanto bien podían ser ellos como la Policía los que custodiasen hasta la práctica de la prueba, sin que en ningún caso se hiciese de espaldas al Juzgado el trasvase de la custodia policial a pericial, obrando en autos (...) escrito (...) el que se pone en conocimiento esa entrega de la Policía a los peritos de todo el material relacionado. Es decir que el Juez de Instrucción conocía que la custodia del material era llevada a cabo por los peritos desde el momento en que dicha custodia se inicia y lo consiente porque así lo había autorizado en al auto de entrada y registro colocando al mismo nivel de intervención a los peritos que a la Policía, porque entendía garantizado el mismo nivel de imparcialidad y así lo cree también esta Sala".

[618] La cuestión quedó definitivamente resuelta tras la STS 179/2006, de 14 de febrero (citada por la jurisprudencia menor, entre otras, SAP Burgos 13/2009, de 9 de marzo), que recoge los principios básicos de recogida de muestras periciales y mantenimiento de la cadena de custodia. Sin perjuicio de venir referida a un supuesto relativo a recogida de restos genéticos y muestras biológicas abandonadas por el sospechoso investigado por parte de la Policía Judicial, en base a la cual fue confeccionada la posterior Pericial biológica que sirvió para la reapertura del Sumario y ulteriormente, en fase de juicio oral, para la condena de los inculpados investigados por su participación en un acto de "kale borroka" o "terrorismo callejero", la citada sentencia contiene conclusiones perfectamente trasladables a la intervención de la Policía Judicial en la confección de todo tipo de pericias, incluidas las de carácter informático. Así resulta interesante la conclusión recogida en la referida sentencia [F.J. 3°], al señalar lo siguiente: "*En el caso que nos ocupa, desde el punto de vista procesal se hacía necesaria la intervención de la policía judicial en la práctica de tal diligencia, bajo la autorización tácita o indirecta del juez, que espera resultados positivos de la investigación de una causa provisionalmente sobreseída. Sólo cuando se aporta un indicio de cargo relevante se puede proceder a la reapertura de las diligencias. La policía, que parte normalmente del peligro o riesgo de pérdida de la muestra o vestigio hallado (art. 236, en relación al 282 LECrim), no puede provocar una revocación del sumario para que el juez controle la práctica de una diligencia que probablemente resulte negativa. La reapertura del sumario sólo podrá producirse ante la existencia de novedades relevantes en el curso de la investigación, en este caso, por resultados*

arts. 126 CE, y 282 y 770 LECrim, debe recordarse que el art. 11.1 Ley Orgánica 2/1986, de Fuerzas y Cuerpos de Seguridad del Estado, atribuye expresamente a los Cuerpos policiales, en su apartado g), la función de "*investigar los delitos para descubrir y detener a los presuntos culpables, asegurar los instrumentos, efectos y pruebas del delito, poniéndolos a disposición del juez o tribunal competente y elaborar los informes técnicos y periciales procedentes".* A *sensu contrario* esta jurisprudencia no puede predicarse en determinadas pericias informáticas si éstas afectan a derechos fundamentales (intimidad, identidad virtual etc..).

Para finalizar el elenco de los posibles sujetos que pueden realizar la pericia, hay que recordar que también es admisible que se designe como peritos a técnicos informáticos de un organismo oficial perjudicado por el delito (STS 1599/1999, de 15 de noviembre)[619] siempre que tuvieran conocimiento las partes a fin de poder ejercitar la recusación si concurre alguna de las causas legales (arts. 416, 464 y 468 LECrim)[620].

También debe mencionarse el supuesto de que subsistan dudas acerca de la fiabilidad del material probatorio. En este caso se podrá acordar la práctica de una pericial para descartar esas dudas y determinar si los archivos informáticos han sido alterados o manipulados (autenticidad e integridad)[621].

---

analíticos positivos y altamente incriminatorios. La lógica estructural de nuestro sistema procesal todavía legitima más si cabe la recogida policial de la muestra".

[619] STS 1599/1999 [FJ 2º] "*el hecho de que los peritos fuesen técnicos informáticos del organismo oficial que había resultado perjudicado no supone obstáculo alguno a la validez de su peritaje. Fueron designados por el juez de instrucción y de dicha designación tuvieron conocimiento las partes que pudieron ejercer la facultad de recusación esgrimiendo alguna de las causas que taxativamente se consignan en el art. 468 LECrim. La circunstancia de que unos peritos pertenezcan a un organismo oficial, que tenga un interés más o menos directo en la causa, no constituye una causa de recusación ya que con ello no se vulnera la necesaria imparcialidad y objetividad requerida a los peritos. Una vez designados por el juez sólo podrían excusarse, según el art. 464 LECrim, si concurriera alguna de las causas comprendidas en el art. 416 del mismo texto legal, que no son otras que, el parentesco y la condición de ser letrado del procesado o acusado. Se trataba de una pericia de gran complejidad técnica y de resultados científicamente fiables, por lo que necesariamente el juez debía encomendársela a conocedores de los sistemas informáticos que habían sido, de alguna manera, intercomunicados aunque de forma externa y absolutamente irregular".*

[620] SAP Valencia 2/2003, de 11 de enero sobre peritos-Inspectores de finanzas en un delito fiscal, STS 499/2004 de 23 de abril, sobre peritos de la CNMV en delitos económicos y ATC 115/2008 de 28 de abril, sobre peritos de organismos oficiales.

[621] SAP Barcelona (sección 7ª) 95/2008, de 29 de enero.

En este sentido, la Sentencia del Tribunal Supremo 300/2015, de 19 mayo dictaminó que para que una conversación entre dos personas mantenida a través de una red social sea considerada como auténtica y pueda ser aceptada como prueba válida en un procedimiento judicial debe ser autentificada por un perito informático en un dictamen pericial informático. Según la sentencia, no es suficiente con presentar como prueba los "*pantallazos*" de la conversación, que son susceptibles de estar manipulados, inclusive hasta el punto de que un único usuario puede simular mantener una conversación en la que realmente se relaciona consigo mismo a través de identidades fingidas, por lo que dichas conversaciones deben ser analizadas por un perito informático y autentificadas en un informe pericial informático al objeto de demostrar su autenticidad. La precitada STS 300/2015, viene a confirmar la necesidad, de contar con la certificación de un dictamen pericial firmado por un perito informático a la hora de autentificar contenidos en redes sociales como Facebook, Twitter, Tuenti o, incluso, cuando se trata de mensajes intercambiados a través de WhatsApp[622].

Centrándonos ya en el objeto de la prueba pericial informática, ésta abarca en una primera y genérica aproximación, el análisis de los equipos informáticos o dispositivos de almacenamiento de datos (discos duros externos, CD-DVD, memorias USB) intervenidos por la Policía y a disposición de la Autoridad Judicial, en el marco del procedimiento penal abierto para la investigación del delito[623].

---

[622] STS 754/2015, de 27 de noviembre, "*la Sala quiere reiterar una idea básica, que ya fue declarada por la STS 300/2015, de 19 de mayo y es que la prueba de una comunicación bidireccional mediante cualquiera de los múltiples sistemas de mensajería instantánea debe ser abordada con todas las cautelas. La posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo. De ahí que la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadasa la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria. Será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido"*

[623] De una forma más descriptiva, VELASCO NÚÑEZ, E. "Delitos cometidos a través de Internet (…) ob. cit. págs. 238 a 240, nos recuerda que la tipología de pericias a realizar sobre los elementos ocupados depende de las necesidades probatorias de los hechos investigados. Así, en ocasiones dependerán del tipo penal perseguido (análisis de los archivos, de los históricos, de los intercambios, de enlaces consultados, del envío de telecomunicaciones informáticas a la víctima, del malware instalado, del rastro dejado para el ataque, el borrado o desaparición del cuerpo del delito y medios empleados para hacerlo, etc.). En otras ocasiones, sin embargo, se complementarán e irán encaminadas a determinar la autoría del ataque (determinación del grado de conocimientos informáticos del investigado para descartar los de otros posibles usuarios compartidos, criterios de búsqueda y materias que usa, nicks vinculados a sus comunicaciones pasadas o actuales -sus interlocutores, fechas, duración, localización, procedencia del último punto de ataque, o rastreo del destino de la información "robada" transmitida), o la intención

La finalidad de la pericial informática, además de servir al juicio de fiabilidad para garantizar la intangibilidad de los archivos informáticos incautados, también servirá para la averiguación del ciberdelito. Su propósito concreto dependerá de lo que se esté investigando, y así, se pueden determinar los siguientes extremos:

- si el software (programa) es el original o una copia no autorizada (ej. si se investigan delitos contra la propiedad intelectual);

- fechas de modificación o creación de los archivos (ej. Si se investiga la posesión y distribución de pornografía infantil);

- origen y destino de la comunicación (ej. si se investigan ataques a la intimidad o al honor por correo electrónico);

- la existencia de daños en el software (virus informáticos).

- análisis de los enlaces consultados e intercambios de archivos (ej. delito de pornografía infantil);

- Seguimiento del rastro de la información robada (ej. revelación de secretos de particulares o de empresa);

- Existencia y en su caso recuperación de archivos ocultos, encriptados o eliminados[624] (ej. daños a sistemas informáticos, revelación de secretos o distribución de pornografía infantil, SAP Madrid (sección 1ª) 531/2010 de 21 de diciembre);

- y cuantos otros análisis exija la investigación del delito[625].

(determinación de palabras vinculadas a la acción penal en el buscador del imputado, inmediatez o no de la acción de borrado, de la de intercambio, cantidad de archivos relacionados con la materia investigada, uso de técnicas de suplantación, anonimato, cifrado, formateo, etc).

[624] AAP Barcelona (sección 15) 46/2006, de 2 de febrero (pericial informática sobre borrado de datos).

[625] Por ejemplo, en el Auto de la AP Castellón (sección 1ª) 367/2010 de 14 de octubre, se acuerda la conveniencia de practicar una pericia informática que aclare las insinuaciones de la Guardia civil sobre si el imputado introdujo un programa "espía" en el ordenador de la fallecida mediante el cual pudiera controlarlo. Y lo justifica diciendo que "analizado el contenido del informe de la Guardia Civil que por testimonio se acompaña, se entiende el interés del imputado por rebatirlo, pues en aquel se concluye, con el refuerzo de la declaración prestada por otra persona, que efectivamente aquel controlaba las actividades de la fallecida y se servía para ello, entre otros medios, de un programa "espía" que habría instalado en su ordenados dentro de una carpeta insertada en noviembre de 2004 y borrada el 22 del mes siguiente. Estas

En un intento de sistematizar lo anterior y siguiendo a MAGRO SERVET[626], de la aplicación práctica del conocimiento específico se desprende la existencia de tres grandes campos de la labor pericial que podrían definirse como:

- pericias de autenticidad,

- pericias de contenido, funcionamiento y recuperación de datos y

- pericias sobre internet.

En el primer caso nos encontramos ante la necesidad de tener a disposición el patrón material de comparación, ya sea de "hard" o "soft", entendido como "indubitable" que permitirá el análisis comparativo determinante de la autenticidad o no del elemento sospechado.

En el segundo ámbito, el espectro es mucho más amplio, pues abarca tan diversos aspectos como el almacenamiento de datos, el análisis y determinación de estructuras de diseño de sistemas, los medios de comunicación y transferencia de datos, método de entrada, acceso, procesamiento y salidas, etc., que en su conjunto requieren la colaboración interdisciplinaria de profesionales en la materia.

Y, en el último, la investigación de ilícitos cometidos a través de la www o bien mediante redes privadas o deep web constituyen un constante desafío para el profesional informático, que le obliga a poseer y mantener permanentemente actualizadas las más modernas herramientas (software) para la detección de intrusiones en sistemas remotos, utilización indebida del correo electrónico, etc.

Todo lo anterior implica que, entre otras actuaciones, pueda requerirse al experto la lectura del contenido de soportes informáticos, la verificación de copia y/o adulteración de sistemas y aplicaciones de software, la impresión del material

---

afirmaciones, de ser ciertas, constituirían un indicio mas de la participación del ahora recurrente en los hechos delictivos origen del proceso, por lo que, siendo que el vaciado del ordenador de aquella no asegura la respuesta a las preguntas que se pretenden responder con la pericia interesada, es menester acceder a la misma por su evidente interés para la causa".

[626] MAGRO SERVET,V. Citado en "La prueba electrónica en el proceso judicial. Ventajas e inconveniente". Facultad de Derecho. Departamento de Criminología: Universidad de Málaga. 15 de marzo de 2013 www.uma.es/criminología/pdf/ponencias.

secuestrado, la impresión del contenido de discos rígidos, establecer el uso indebido de marcas o la explicación de uso de utilitarios y/o sistemas de computación, etc.

Al acto pericial en el caso de que no pueda ser reproducible en el juicio oral, que será lo normal para las informáticas, pueden (no es obligatorio, sino potestativo) concurrir con su representación, tanto las partes acusadoras personadas como la defensa (art. 476 LECrim). De esta manera, una vez puesta en conocimiento de las partes personadas la resolución judicial por la que se acuerde la confección de la pericia, será la parte interesada la que deba solicitar la asistencia a la práctica de la pericia. Para la práctica de esta diligencia de preconstitución probatoria el art. 477 LECrim indica que "*asistirá siempre el secretario que actué en la causa*". Al no ser reproducible en el juicio oral deberá estar presente el LAJ para tener plena validez probatoria. También se podrá practicar como anticipada, a propuesta de las partes si se teme que no va a poder practicarse en juicio oral o va a motivar una suspensión.

Por otro lado, las partes personadas en la causa pueden potenciar sus facultades de participación en la elaboración de la pericia durante la fase de instrucción mediante la emisión de sus observaciones durante su realización (art. 480 LECrim), sin perjuicio de que la pudieran contradecir e interrogar sobre ella a la hora de la emisión de sus conclusiones por parte de los peritos al ratificarlas en el Juzgado (art. 483 LECrim), o de aportar una contrapericia propia diferente o coincidente.

Las distintas operaciones periciales deben plasmarse en el correspondiente informe pericial (art. 478 LECrim), que debe comprender: la descripción del objeto del mismo modo o estado en que se halle, una relación detallada de todas las operaciones que practicadas y su resultado, así como las conclusiones que en vista de tales datos formulen los peritos conforme a los principios y reglas de su ciencia y arte.

En el juicio oral no es necesario proponerla en los escritos de calificación. En el ordinario puede acordarla también el Tribunal de oficio si la considera necesaria para comprobar algún hecho (art. 729.2 LECrim). En el abreviado, las partes también pueden proponerla al inicio del juicio oral.

Será necesaria su práctica en juicio oral, salvo en los supuestos de prueba preconstituida o anticipada. En estos casos se aportará como documental y será

evaluable en sentencia sin necesidad de ratificarse en juicio el perito. Sólo cuando alguna de las partes lo impugne en el escrito de conclusiones, el perito deberá ser traído al juicio a ser sometido a contradicción (STS 1281/2006, de 27 de diciembre).

La necesaria intervención de dos peritos en el sumario dispuesta por el artículo 459 LECrim se ha atemperado por la jurisprudencia en el caso de los laboratorios oficiales, en base al artículo 788.2 LECrim (informes científicos realizados por los especialistas de los laboratorios oficiales del Estado, basados en conocimientos especializados, que no precisan de ratificación para ser valorados, salvo en caso de impugnación tempestiva y con contenido material) y se ha planteado la posibilidad de que dicha previsión legal se aplique extensivamente a otras pruebas periciales de naturaleza análoga.

A este respecto, el Acuerdo del Pleno no jurisdiccional de la Sala Segunda del Tribunal Supremo de 21 de mayo de 1999 interpretó que "la exigencia de duplicidad de peritos en el procedimiento ordinario queda cumplida cuando el peritaje se lleva a cabo por un laboratorio oficial y el dictamen se refiere a criterios analíticos". Tal criterio se ha consolidado en las sentencias posteriores. Como ejemplo, las SSTS 113/2009, de 12 de febrero y 1302/2005, de 8 de noviembre señala [FJ1º]: "*Precisamente, por las condiciones de laboratorio público, dotado de la imparcialidad que caracteriza la función de la administración pública, y por la naturaleza oficial del laboratorio, que incorpora a varios profesionales que trabajan en el mismo, la jurisprudencia de esta Sala ya admitió que los informes periciales firmados por una persona, como responsable del laboratorio oficial, rellenaban la exigencia de pluralidad de peritos que exige el art. 459 para las causas tramitadas en el procedimiento ordinario por delitos"*[627].

[627] Doctrina que ha sido recogida en otras resoluciones, como las SSTS 1081/2004, de 30 de septiembre, y 1365/2003, de 17 de octubre, que, muy clarificadoramente, señala [FJ3º] que *"Tiene declarado esta Sala, como es exponente la Sentencia 806/1999, de 10 de junio, que la exigencia de dualidad de peritos en cada dictamen pericial obedece a la mayor garantía de acierto que representa la posible coincidencia de pareceres de dos peritos frente a la opinión única, y a las mejores condiciones de objetiva valoración que para el Tribunal representan las posibles divergencias y opiniones encontradas de dos peritos intervinientes. De lo que se trata es de reforzar la eficacia, el acierto y el rigor técnico de los dictámenes periciales, sin que por ello se haga de la dualidad de peritos una condición inexcusable de la necesaria garantía puesto que el párrafo segundo del propio art. 459 exceptúa el caso de que no hubiese más de un perito en el lugar y no fuera posible esperar la llegada de otro sin graves inconvenientes para el curso del sumario. En todo caso si el fundamento de la exigencia se halla en la mayor probabilidad de acierto que representa el trabajo realizado por varios, la finalidad de la norma queda satisfecha en el caso de*

La actuación en juicio de un solo perito no afecta a la validez de la prueba ni tampoco vulnera la tutela judicial efectiva si no produce indefensión[628].

Por último, cabe la posibilidad de intervención pericial por videoconferencia (arts. 325 y 731 bis LECrim), para la emisión, ratificación y sometimiento a contradicción, cuando concurran razones de utilidad, seguridad u orden público o cuando la comparecencia resulte gravosa o perjudicial para los peritos.

4. INCORPORACIÓN AL PROCESO DEL MATERIAL PROBATORIO INFORMÁTICO.

4.1 Consideraciones generales.

Como regla general, se puede afirmar que sólo tienen la consideración de pruebas aquellas que se han practicado en el acto del juicio oral. Es en esta fase procesal cuando las pruebas se practican con plena observancia de los principios de publicidad, oralidad, inmediación y contradicción, y con el debido respeto a los derechos

---

dictámenes periciales emitidos por Órganos Oficiales dotados de equipos técnicos altamente cualificados integrados por distintos profesionales que intervienen como tales participando cada uno de sus miembros en el trabajo común dentro de la división de tareas o funciones. En tales casos el mero dato formal de estar suscrito el informe por uno solo de los profesionales del equipo –normalmente el que ejerce facultades representativas del Laboratorio u Órgano informante, como 'Responsable" o "Jefe" del Servicio de que se trate– no puede ocultar que el dictamen no es obra de un solo individuo, es decir, de un perito, sino del trabajo en equipo normalmente ejecutado según procedimientos científicos protocolizados en los que intervienen varios expertos, desarrollando cada uno lo que le compete en el común quehacer materializado por todos. En estos casos no es que no sea aplicable el art. 459 de la Ley de Enjuiciamiento Criminal sino que debe entenderse satisfecha la exigencia que el precepto contiene".

[628] Doctrina recogida por la jurisprudencia menor, pudiendo citarse la SAP de Madrid (sección 29) 96/2011, de 8 de noviembre que recogiendo el acuerdo del Pleno no jurisdiccional de la Sala Segunda de 21 de mayo de 1999 afirmó la innecesariedad de ratificación del dictamen de los peritos integrados en organismos públicos, salvo que la parte a quien perjudique impugne el dictamen o interese su presencia para someterlos a contradicción en el plenario y lo hiciera en momento procesal oportuno, establece que "es el caso de los informes científicos realizados por los especialistas de los Laboratorios oficiales del Estado, basados en conocimientos especializados, que no precisan de ratificación para ser valorados, salvo en caso de impugnación tempestiva y con contenido material (SS. 21.1.2005 en relación con informes lofoscópicos y de 27.11.2000 en cuanto a informes de Gabinete de Balística). Como justificación, se invoca la condición de funcionarios públicos de quienes los elaboran, la consiguiente presunción de imparcialidad, su especialización técnica, y adscripción a organismos dotados de los costosos y sofisticados medios propios en las modernas técnicas de análisis y la doctrina del Tribunal Constitucional en relación con la denominada "prueba preconstituida".

fundamentales del inculpado a no declarar contra sí mismo y a no confesarse culpable (art. 24.2 CE).

No obstante lo dicho, la regla general de que la prueba en el proceso penal únicamente tiene lugar en la fase del juicio oral admite excepciones, ya sea por la posibilidad de practicarse en momento distinto, ya sea por la imposibilidad de su repetición, como son los supuestos de prueba anticipada y prueba preconstituida.

Se señala por la doctrina[629] que a diferencia de otras fuentes de prueba, como los documentos en papel o las piezas de convicción consistentes en objetos materiales que revelan los restos o las huellas del delito, los útiles informáticos no mantienen una relación unívoca con un solo medio de prueba. Por el contrario, las informaciones que contienen pueden incorporarse al proceso a través de diferentes medios de prueba, e incluso un mismo material puede ser propuesto para la práctica de la prueba de diferentes medios, fundamentalmente como documental o reconocimiento judicial. Por ejemplo, intervenido un ordenador con archivos de textos, podrá optarse por proponer el reconocimiento judicial del mismo, iniciando el equipo y accediendo el Juez o Tribunal a los diferentes archivos de texto. O podrán obtenerse documentos en papel, imprimiendo el texto de dichos archivos y proponiendo prueba documental, consistente en el documento obtenido en papel. Si se trata de imágenes podrán imprimirse también en papel, procediéndose a su unión a la causa en esta forma o podrán apreciarse las imágenes en pantalla por el Juez o Tribunal abriendo los archivos respectivos. Los archivos de sonido podrán en su caso ser además transcritos. La modalidad de uso de las informaciones contenidas en la memoria informática habrá de decidirse caso por caso. Deberá tenerse en cuenta que con frecuencia las Audiencias Provinciales o los Jueces de lo Penal querrán disponer en el juicio de documentos en papel que reflejen fielmente las imágenes o transcriban las palabras, o que sean la impresión en papel de los textos. En ocasiones puede ser indispensable que el Juez o Tribunal aprecie directamente imágenes en pantalla, pero en otras ocasiones, la apreciación o lectura en pantalla no añadirá nada y quizás entorpecerá o retrasará algo el juicio. Además, los archivos informáticos pueden dañarse, alterarse o borrarse por un uso descuidado o simplemente por avería en

[629] DE JORGE MESAS, L. F. *La incorporación de las nuevas tecnologías informáticas y de telecomunicaciones al proceso penal* en "Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia" (Velasco Núñez, Coord). Cuadernos de derecho judicial, Consejo General del Poder Judicial, Madrid 2007. págs. 358 a 365.

el equipo. Por el contrario, las imágenes o los textos en papel adquieren fijeza y son menos vulnerables al deterioro o pérdida.

Otro ejemplo de aportación de material informático al acto del juicio oral es el de las escuchas telefónicas, cuya forma de aportación puede hacerse extensiva al resto de medidas de investigación tecnológica, al constituir en realidad una prueba preconstituida que, como todas las pruebas de esta naturaleza, requiere ser introducida en el juicio oral en condiciones de inmediación, publicidad y contradicción. Como requisitos esenciales para la validez de esta prueba, señala el Tribunal Supremo los siguientes (STS 513/2010, de 2 de junio [FJ 2º]:

"1) La aportación de las cintas;

2) La transcripción de las mismas, bien integra o bien de los aspectos relevantes para la investigación, cuando la prueba se realice sobre la base de las transcripciones y no directamente mediante la audición de las cintas;

3) El cotejo bajo la fe del LAJ de tales párrafos con las cintas originales, para el caso de que dicha transcripción mecanográfica se encargue -como es usual- a los funcionarios policiales;

4) La disponibilidad de este material para las partes.

5) Y, finalmente, la audición o lectura de las mismas en el juicio oral, que da cumplimiento a los principios de oralidad y contradicción, previa petición de las partes, pues si estas no lo solicitan, dando por bueno su contenido, la buena fe procesal impediría invocar tal falta de audición o lectura en esta sede casacional.

Ahora bien, la audición o lectura no agotan las formas de introducción de las escuchas telefónicas en juicio, ya que es posible introducirlas, incluso, mediante el testimonio de los agentes policiales encargados de las mismas y, en este sentido, señala la STS 112/2012, de 23 de febrero [FJ 2º], que *"conviene recordar que ni la jurisprudencia constitucional ni esta misma Sala han exigido como presupuesto de validez ni de suficiencia probatoria que las cintas hayan sido objeto de audición en el plenario. Con carácter general, la escuchas, debidamente autorizadas, sometidas a control judicial e inspiradas en los principios de necesidad, excepcionalidad y*

proporcionalidad, serán susceptibles de valoración jurisdiccional siempre que puedan convertirse en verdadera prueba. En efecto, las SSTS 363/2008, 23 de junio, 1778/2001, 3 de octubre y 807/2001, 11 de mayo, precisan que el contenido de esas escuchas, como medio de prueba plena en el juicio deberá ser introducido en el mismo regularmente, bien mediante la audición directa del contenido de las cintas por el Tribunal, fuente original de la prueba, mediante la lectura en el juicio de las transcripciones, diligencia sumarial documentada, previamente cotejadas por el Secretario con sus originales, e incluso por testimonio directo de los agentes encargados de las escuchas, criterio también reiterado en las SSTS 1070/2003, 22 de julio y 112/2002, 17 de junio".

Otra de las posibilidades que nuestra jurisprudencia admite para la introducción de las escuchas telefónicas en juicio es su aportación como prueba documental que, en el caso de que se dé por reproducida, no solicitando ninguna de las partes su audición, será perfectamente valorable por el Tribunal[630]. Así, la STC 26/2010, de 27 de abril, señalaba que "*también hemos concluido que para dicha incorporación por vía documental no es requisito imprescindible la lectura de las transcripciones en el acto del juicio, siendo admisible que se dé por reproducida, siempre que dicha prueba se haya conformado con las debidas garantías y se haya podido someter a contradicción y que tal proceder, en suma, no conlleve una merma del derecho de defensa*", señalando más adelante que "*la no audición de las cintas en el juicio, así como que el Secretario no adverara la transcripción de las mismas, no supone, sin más, que las grabaciones no puedan ser valoradas por el Tribunal sentenciador. En efecto, las grabaciones telefónicas tienen la consideración de prueba documental (documento fonográfico) por lo que pueden incorporarse al proceso como tal documental, aunque la utilización de tal medio probatorio en el juicio puede hacerse, de maneras distintas. Ahora bien, el hecho de que las grabaciones puedan reproducirse en el acto del juicio oral y someterse a contradicción por las partes, bien de modo directo, mediante la audición de las cintas, bien indirectamente con la lectura de las transcripciones no significa que la prueba documental fonográfica carezca de valor probatorio en los supuestos en los que haya sido incorporada como prueba documental y haya sido dada por reproducida sin que nadie pidiera la audición de las cintas o la lectura de su transcripción en la vista oral"* (en el mismo sentido la STS 789/2011, de 20 de julio).

[630] STS 315/2012, de 22 de marzo [FJ 1º].

Lo esencial para una válida introducción de la grabación de las comunicaciones en el juicio oral es que se respete el principio de contradicción y el derecho de defensa del acusado. Por ello, otra posible forma de introducir su contenido viene constituida por el interrogatorio a los acusados acerca del contenido de las comunicaciones, permitiéndoles de este modo conocer la prueba y articular su defensa frente a ella. Así, la STS 285/2011, de 20 de abril, establece que "*consecuentemente se trata de transcripciones avaladas por la fe pública del Secretario Judicial tras la audición de las cintas originales, sin que las partes hicieran constar en momento procesal oportuno, oposición o contradicción alguna, y cuyo contenido fue introducido, de forma expresa en el acto del juicio oral, al hacer pormenorizado y detallado interrogatorio, a cada uno de los interlocutores, respecto de las conversaciones concretas, con expresión de día, hora y contenido de las mismas"*.

La falta de audición no tiene por qué generar indefensión. Si estando las grabaciones originales o sus transcripciones a disposición de las partes durante el juicio estas no solicitan su lectura o reproducción, cuestionando de algún modo su contenido, no se genera ningún tipo de indefensión que pueda afectar a la validez de la prueba, y así la STS 867/2014, de 11 de diciembre establece que "*ya en la citada STC 128/1988, llegamos a idéntica conclusión bajo el argumento de que no habiéndose impugnado en todo o en parte la transcripción de las cintas, y habiéndolas dado por reproducidas, no se le puede negar valor probatorio a tales transcripciones". "No habiéndose pedido ni en el juicio oral ni en la apelación la audición de las cintas no puede el querellado - argumenta el TC - quejarse de indefensión. Es cierto que él no tiene que probar su inocencia, pero también lo es que si, conocedor de unas pruebas correctamente aportadas y de cuyo contenido puede derivarse un resultado probatorio perjudicial para él, no se defiende de ellas por falta de diligencia o por haber elegido una determinada estrategia procesal, no puede quejarse de indefensión que, en este caso, ciertamente no se ha producido". Esta doctrina ha sido acogida y remarcada también en la jurisprudencia al ser cuestionada la forma de operar en el plenario esas diligencias de investigación* (STS 85/2011, de 7 de febrero; STS 565/2011, de 6 de junio; y STS 715/2013, de 27 de septiembre, entre otras)".

En definitiva, y aplicando lo anterior a la incorporación del material probatorio informático en el acto del juicio oral, pueden establecerse tres maneras: como prueba documental, como testifical o como pericial.

1) Como prueba documental.

En la actualidad en el proceso penal, la prueba documental ha adquirido una mayor trascendencia, tanto por el desarrollo de las denominadas nuevas formas de delincuencia (delitos fiscales, contable, urbanísticos, sociopolíticos), en los que el recurso a la prueba documental es imprescindible, como por la aparición de nuevas técnicas de reproducción (videográficas, magnetofónicas...) que amplían el propio concepto de prueba documental. Ello ha producido una desfiguración del tópico que afirmaba que el proceso civil es el reino del documento, mientras que el penal lo es del testigo, dado el espectacular desarrollo de las nuevas tecnologías[631].

La información puede ser presentada ante el órgano judicial mediante la aportación del propio sistema o equipo de almacenamiento, que será reproducido y examinado por el tribunal (como prueba documental de conformidad con el art. 726 LECrim) con los medios técnicos que resulten necesarios, y que frecuentemente estarán a disposición del órgano judicial (por ejemplo, ordenador para la lectura de dispositivos USB o de DVD, dotado del programa informático adecuado para el concreto formato de archivo de que se trate).

También puede realizarse mediante la incorporación al proceso de una copia de la información del mismo que sea relevante para el proceso (volcado), pues únicamente han de ser ocupados aquellos dispositivos que resulten estrictamente necesarios para la tramitación del proceso (art. 588 sexies c LECrim), procediendo en otro caso únicamente a la ocupación de los datos.

En otras ocasiones será necesaria la realización de un análisis de la información del sistema o equipo que solamente puede ser afrontada con conocimientos

[631] DE URBANO CASTRILLO, E. *El documento electrónico: aspectos procesales*, en "Internet y Derecho Penal", Escuela Judicial CGPJ, 2001, pág. 555.

especializados en la materia, a través de la práctica de un dictamen de peritos o prueba pericial informática que actuará sobre una copia o clonado de los datos[632].

También debe tenerse en cuenta a éste respecto el artículo 38 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[633](LUTICAJ), a cuyo tenor,

"1. La presentación de toda clase de escritos, documentos, dictámenes, informes u otros medios o instrumentos se ajustará a lo dispuesto en las leyes procesales, debiendo ir acompañados en todo caso del formulario normalizado a que se refiere el apartado 4 del artículo 36, en el que además se consignará el tipo y número de expediente y año al que se refiera el escrito.

2. En todo caso, la presentación de escritos, documentos y otros medios o instrumentos se ajustará a las siguientes reglas:

a) Los documentos en papel que, conforme a lo dispuesto en las leyes procesales puedan o deban ser aportados por las partes en cualquier momento del procedimiento, deberán ser incorporados como anexo al documento principal mediante imagen digitalizada de la copia, si fueran públicos, o del original del documento obrante en papel, si se tratara de documentos privados. El archivo de la imagen digitalizada habrá de ir firmado mediante la utilización de los sistemas de firma electrónica previstos en la presente Ley, en las leyes procesales o en otras normas de desarrollo.

b) Los documentos electrónicos públicos o privados se incorporarán como anexo al documento principal siguiendo los sistemas previstos en esta Ley o en sus normas de desarrollo y conforme a lo previsto en la Ley 59/2003, de 19 de diciembre, de firma electrónica.

c) En caso de que fueran impugnados por la parte contraria, se procederá conforme a lo dispuesto en las leyes procesales y, en su caso, en la Ley 59/2003, de 19 de diciembre, de firma electrónica.

[632] DELGADO MARTIN, J. "La prueba electrónica en el proceso penal". ob. cit. pág. 4.

[633] *Vid.* SANCHÍS CRESPO, C. en *La prueba en soporte electrónico*, ob. cit. pág. 717.

d) No se admitirá la aportación en otra forma, salvo en el supuesto de que, por las singularidades características del documento, el sistema no permita su incorporación como anexo para su envío por vía telemática. En estos casos, el usuario hará llegar dicha documentación al destinatario por otros medios en la forma que establezcan las normas procesales, y deberá hacer referencia a los datos identificativos del envío telemático al que no pudo ser adjuntada, presentando el original ante el órgano judicial en el día siguiente hábil a aquel en que se hubiera efectuado el envío telemático. Tales documentos serán depositados y custodiados por quien corresponda en el archivo, de gestión o definitivo, de la oficina judicial, dejando constancia en el expediente judicial electrónico de su existencia únicamente en formato papel. Cuando se deban incorporar documentos sobre los cuales existan sospechas de falsedad, deberá aportarse en todo caso además el documento original, al que se le dará el tratamiento contemplado en el párrafo anterior.

e) En los casos en que se deban aportar al procedimiento medios o instrumentos de prueba que por su propia naturaleza no sean susceptibles de digitalización, serán depositados y custodiados por quien corresponda en el archivo de gestión o definitivo de la oficina judicial, dejando constancia en el expediente judicial electrónico de su existencia".

La prueba en soporte informático, por su encuadre en la prueba documental penal, puede acceder al proceso, y más en concreto, al acto del juicio oral, a través de tres vías: lectura, examen por el propio Tribunal e, indirectamente, a través de una pericia documental.

A) Lectura.

En los supuestos de prueba anticipada y preconstituida, así como en general, en todos aquellos casos en los que las diligencias sumariales fueron practicadas con todas las garantías, pero que por algún motivo ya no pueden ser practicadas en el juicio oral, se prevé por el artículo 730 LECrim la posibilidad de dar entrada en el juicio mediante

la reproducción por lectura[634]. Incluye la reproducción de videos, CDS, etc. En este caso, se ha dicho que la prueba tiene analogía con el examen directo del Juez (art. 726 LECrim)[635].

Ahora bien, si las partes disponen de una copia de la grabación o de la transcripción escrita no es necesario su reproducción en juicio o al menos no de todo el contenido, debiendo limitarse a aquellos pasajes o extremos de su interés.

B) Examen por el propio Tribunal.

Constituye la posibilidad de que sea el propio órgano jurisdiccional el que examine *ex officio* las pruebas documentales existentes en autos no propuestas por las partes. Es decir, se plantea la posibilidad de que el órgano sentenciador, en el juicio oral, tome la iniciativa de incorporar al acervo probatorio, alguna documental por considerar necesario su concurso, a fin de procurar obtener la "verdad material".

El hecho de que no rija en el procedimiento probatorio penal, el principio de aportación de parte, así como la posición neutral del propio Tribunal, permiten sostener tal posibilidad. Cabe, por tanto, que el órgano judicial examine pruebas existentes en autos, no propuestas por las partes- por olvido o no interés- y las que declare de necesaria práctica para comprobar algún extremo del factum del escrito de calificación.

---

[634] Art. 730 LECrim: "*Podrán también leerse a instancia de cualquiera de las partes las diligencias practicadas en el sumario, que, por causas independientes de la voluntad de aquéllas, no puedan ser reproducidas en el juicio oral".*

[635] MEDRANO I MOLINA J. M. La práctica de la prueba por soportes informáticos y audiovisuales en el proceso penal. Universidad de Valencia. Pág. 8 y 9. http://docplayer.es/7251978-La-practica-de-la-prueba-por-soportes-informaticos-y-audiovisuales-en-el-proceso-penal.html
Algunas razones que pueden justificar el empleo de esta disposición pueden ser, por ejemplo, en el caso de una prueba testifical: Que el testigo haya fallecido. Se encuentra en el extranjero, fuera de la jurisdicción del Tribunal no siendo factible su comparecencia. Se encuentra en paradero desconocido, habiendo resultado infructuosas las diligencias practicadas para su citación en forma legal y fallidas las gestiones realizadas para su localización. En definitiva, como señala DE URBANO CASTRILLO se trata de convertir en auténticas pruebas, para lo que deben practicarse en el plenario, lo que se trae del sumario, venga en el estado que venga (mera diligencia de investigación, prueba anticipada o preconstituida). Las nuevas tecnologías han abierto un amplio campo para que mediante este artículo, hayan accedido a la vista oral pruebas documentales con los soportes más variados, a través de su reproducción mediante aparatos e ingenios técnicos al efecto (videos, cintas magnetofónicas....) que efectúan su *lectura*, es decir, la interpretación de los signos visuales o sonoros que las componen. Así lo han contemplado expresamente los arts. 777.2 y 797.2 LECrim, para el supuesto de las declaraciones de testigos documentadas en soporte apto para la reproducción de la imagen y el sonido.

Para ello el Tribunal no necesita contar con el asentimiento de las partes para la recepción de la prueba y no está obligado a escuchar el parecer de las mismas sobre su decisión, que se fundamenta en el llamado "principio de oficialidad" y viene amparado por el art. 729.2 LECrim y por una extensa jurisprudencia (STS 22 de enero de 1992, STS 904/1995 de 23 de septiembre, STS 1186/2000 de 28 junio, STS 2389/2001, de 14 diciembre, STS 1482/2002 de 17 septiembre, STS 199/2011, de 30 de marzo, entre otras).

La iniciativa que al Tribunal atribuye el art. 729.2 de la LECrim puede ser considerada como "prueba sobre la prueba", que no tiene la finalidad de probar hechos favorables o desfavorables sino de verificar su existencia en el proceso, desde la perspectiva del art. 641 de la LECrim, por lo que puede considerarse neutral y respetuosa con el principio acusatorio, que impone la carga de la prueba a la acusación. Su compatibilidad con la imparcialidad del Tribunal ha sido reconocida por la STC 187/2000, de 10 de julio. Debe reunir determinadas condiciones: que sea una prueba neutral, que clarifique una cuestión dudosa, que se permita a las partes proponer prueba, que se someta a contradicción y que no sea la única de cargo. Tal prueba puede complementarse con la pericial y con la testifical, en orden a acreditar que son auténticas las manifestaciones grabadas (que no han sido manipuladas) o que son veraces la imágenes de un video o de un archivo informático, o se corresponde la voz grabada con la de la persona a la que se atribuye.

En todo caso, si se trata de la aportación del contenido de correos electrónicos, cuyo conocimiento se produce por lo general, a través de su reflejo impreso, se requerirá que la parte que los pretenda hacer valer los aporte, si no antes, al menos en el acto del juicio. Así lo dispone la SAP Valladolid 549/2002, de 22 de julio en un supuesto en el que niega la posibilidad de su presentación posterior, en concreto en la tramitación del recurso de apelación.

C) Indirectamente, a través de una pericia documental.

La prueba pericial informática en la inmensa mayoría de los supuestos se encontrará incardinada en lo que es la prueba documental, donde, a tenor de la LECrim

(art. 726), es el Tribunal el que examinará por sí mismo los documentos a que se refiere dicha prueba, pero en ningún momento se prohíbe que dicho examen venga auxiliado por el personal técnico oportuno que clarifique o ayude a comprender el significado de tales documentos, de conformidad con lo prevenido en el art. 230.1 LOPJ, por lo que en determinados supuestos de carácter complejo, será prácticamente imprescindible el apoyo externo en cuanto a la comprensión de los datos o incluso la mera conexión o ejecución del programa que los contenga.

Es por ello que en la práctica procesal la jurisprudencia ha convertido el dictamen pericial en prueba preconstituida documental, perfectamente evaluable en sentencia sin ratificación en el acto del plenario, e invirtiendo la carga de su impugnación[636]. Obliga a quien lo cuestione a expresar en su escrito de conclusiones, para posibilitar la contradicción a la contraparte y demostrar la buena fe de la real necesidad de aclarar o complementar la pericia, los motivos concretos de su discrepancia (disconformidad con el resultado de la pericia, contraanálisis privado diverso, disconformidad con la competencia o imparcialidad del perito), para permitir el sometimiento final al perito a contradicción en el plenario[637] (doctrina recogida, entre otras, en SSTC 127/1990 de 5 de julio [FJ4º], 24/1991 de 11 de febrero [FJ3º] y SSTS 1642/2000, de 23 de octubre, 1281/2006, de 27 de diciembre, Acuerdo del Pleno no jurisdiccional de 21 de mayo de 1999, confirmado por el Acuerdo de 23 de febrero de 2001).

2) La segunda forma de incorporar el material probatorio es a través de la prueba *testifical:* de la persona que ha tenido contacto con el material original, que deberá explicar contradictoriamente en el acto de la vista para adverar los extremos que se

[636] STC 24/1991 de 11 de febrero [FJ3º]. Estas pericias (referida a una pericial técnica que acompaña a un atestado) practicadas necesariamente con anterioridad a la celebración del juicio, e incluso con antelación al inicio del proceso latu sensu entendido constituyen pruebas preconstituidas que despliegan toda su validez si no son impugnadas por ninguna de las partes y son aportadas al acervo de diligencias.

[637] STS 11 de noviembre de 1996 (rec. 113/1996)[FJ2º] "*Los dictámenes e informes emitidos por Centros e Instituciones oficiales gozan de la garantía de imparcialidad, objetividad y solvencia que, en principio, ha de reconocerse a los mismos, por lo cual, salvo que alguna de las partes interese expresamente la ratificación de los técnicos informantes, la ampliación por los mismos de extremos determinados, la práctica de análisis contradictorios o la presencia de los peritos oficiales junto con otros de designación particular en el juicio oral, por motivos debidamente justificados, no se considera preciso ni la ratificación de los mismos ante la autoridad judicial, ni la presencia de los peritos en la vista del juicio oral".*

debatan, introduciéndolo de esa forma en el proceso, con el inconveniente de generar un grado de convicción menor, seguramente, que si se tuviese delante el soporte original[638].

3) Por último, como prueba *pericial:* por quien habiendo tenido contacto con el material probatorio, haya emitido informe técnico sobre cualquier extremo sometido a debate respecto de determinado inculpado, con base a la información manejada cuya fuente o procedencia, si es discutida, debe concretar y ratificar para validar su elaboración y detalles, si los precisa cualquier parte, permitiendo así su introducción contradictoria en el proceso[639].

Es evidente que en la prueba del ciberdelito será en muchos casos imprescindible el concurso de peritos informáticos, para que a través de sus conocimientos específicos se pueda acreditar el contenido de determinados soportes por sus especiales características.

Simplemente recordemos el caso de los documentos electrónicos borrados o protegidos por una contraseña, sin la cual no se llegaría a acceder a la información relevante que podrá constituir posteriormente una prueba incriminatoria decisiva.

También cuando se trata de verificar la localización desde la que se han remitido determinados correos electrónicos (SAP Valencia, 322/2002 de 8 julio) aunque en muchos supuestos, este dato no será suficiente para poder realizar un pronunciamiento condenatorio, dadas las exigencias necesarias para desvirtuar la presunción de inocencia (SAP Cáceres, 127/2002 de 30 diciembre 2002). O bien aquellos supuestos en los que se solicita la reproducción de un soporte audiovisual respecto del cual, se requieren actuaciones accesorias que permitan la reconstrucción del sonido o la imagen, ya sea por posibles defectos sufridos en el soporte, o por la naturaleza inherente del mismo.

---

[638] SAP Las Palmas (sección 2ª) 180/2011, de 15 de julio que confirma una condena basada en la declaración de testigos, uno de ellos ex novio de la denunciante, quien sostiene haber mantenido la conversación mediante WhatsApp y otra testigo que al parecer vio en Facebook los comentarios injuriosos, y sin haberse acreditado la titularidad de la cuenta, del perfil y del número de teléfono asociado al WhatsApp desde los que se remitieron los mensajes presuntamente denunciados.

[639] STS 342/2013, de 17 de abril [FJ 2º] "*la verdadera fuente probatoria, el genuino material incriminatorio sobre el que se sustenta la condena no está encerrado en el CD al que se refiere el recurrente, sino en el informe pericial acerca de la existencia, autenticidad y contenido de las conversaciones mantenidas por el acusado con sus víctimas. Y este dictamen pericial, fue objeto de debate, filtrado por el principio de contradicción en el plenario, habiendo aportado la defensa su propio perito informático para contradecir cuantas conclusiones técnicas aparecían allí proclamadas".*

En todo caso, las nuevas tecnologías vienen a suponer un forzoso reciclaje y adaptación de los peritajes realizados tradicionalmente por los equipos de Policía Científica respecto de elementos caligráficos en papel[640].

4.2 Aportación de la prueba informática por las partes.

Muy brevemente y a este respecto cabe recordar que durante la fase de instrucción cualquiera de las partes puede, en primer lugar, aportar una "*prueba*" informática al proceso solicitando la unión a los autos del propio dispositivo en el que se encuentre la misma, pudiendo también acompañar una copia en papel con la transcripción de la información relevante. En segundo lugar, puede solicitar al Juez que reclame la remisión de una prueba o documento electrónico, designando oportunamente el lugar o archivo en el que se encuentre. Asimismo se podrá practicar algún dictamen pericial sobre la mencionada prueba informática, ya sea a instancia de parte o porque el Juez considere necesario realizarla de oficio o a la vista de las alegaciones de impugnación de la otra parte.

Posteriormente, la parte interesada podrá introducir la prueba informática en el juicio oral proponiéndola como prueba documental que, una vez admitida, será objeto de examen por el tribunal al amparo del art. 726 LECrim, insertándose en el debate procesal con sometimiento a la contradicción de las partes, quienes podrán impugnar su contenido, su forma de acceso al proceso y sus condiciones de autenticidad e integridad.

Respecto a las pericias particulares, hay que señalar que cada vez resulta más frecuente que determinadas denuncias o querellas, especialmente en el ámbito de los delitos de propiedad intelectual e industrial, vengan acompañadas de un dictamen pericial informático para aportar al Juzgador mayores datos para valorar la realidad de la actividad presuntamente delictiva denunciada, y, en consecuencia, motivar la petición

[640] MEDRANO I MOLINA J. M. La práctica de la prueba por soportes informáticos y audiovisuales en el proceso penal. Universidad de Valencia. Pág. 10. http://docplayer.es/7251978-La-practica-de-la-prueba-por-soportes-informaticos-y-audiovisuales-en-el-proceso-penal.html 3/1/17 a las 21.30

de diligencias que suelen interesarse en la propia denuncia o querella, o bien posteriormente en el curso del procedimiento, una vez incoado el mismo[641].

Ahora bien, dicha práctica procesal puede encontrarse con importantes problemas tanto en lo relativo al juicio de fiabilidad del material objeto de pericia, con evidentes efectos de merma en cuanto a la eficacia pretendida por la pericia, como en lo atinente a la posible ilicitud o nulidad de la prueba pericial practicada si la misma, siendo ajena al control jurisdiccional, llega a afectar de algún modo a derechos fundamentales.

La primera de las cuestiones planteadas deriva de la evidente dificultad para el denunciante particular de acreditar que el aseguramiento del objeto de la prueba pericial informática ha sido practicado con todas las garantías exigibles para impedir cualquier alteración o manipulación del mismo, cuando no se cuenta todavía con la intervención judicial/policial que permita dotar de cierta oficialidad a la labor de conservación. Sería más aconsejable, desde el punto de vista de la eficacia probatoria, acudir desde el primer momento a mecanismos de intervención de fedatario público (actas notariales), e incluso al inmediato depósito de los elementos que serán objeto de pericia particular ante la autoridad policial. En otro caso la eficacia de la prueba se verá seriamente reducida[642]. Otra posibilidad sería solicitar al Juzgado que acuerde tras recibir la denuncia una nueva pericial de contraste, esta vez sí revestida de las garantías propias

[641] En muchos de estos casos la denuncia, en lugar de presentarse directamente ante el Juzgado, se dirige a la correspondiente Brigada o Grupo de investigación policial especializado en delincuencia telemática, que, tras las comprobaciones y diligencias oportunas, confecciona el correspondiente atestado incorporando la denuncia interpuesta por particulares o personas jurídicas como anexo, e interesando del Juzgado la incoación del oportuno procedimiento, y paralelamente, como primera diligencia a practicar, a fin de asegurar las fuentes de prueba reveladoras de la presunta actividad delictiva, la solicitud de entrada y registro en domicilio o sede social de empresa vinculada al denunciado.

[642] En este sentido, el Auto de la Audiencia Provincial de Vizcaya (Sección 2ª) 175/2008, de 31 de marzo. en un supuesto de investigación de un presunto delito contra la propiedad intelectual, por presunta apropiación por los denunciados, ex directivos y ex empleados de la empresa denunciante, de determinadas aplicaciones informáticas de elaboración interna de la empresa, así como de determinadas plataformas y programas informáticos sobre los que la empresa denunciante poseía licencia para su exclusiva distribución en España, si bien la denuncia aparece acompañada de dictamen pericial, señala que "*respecto de la prueba pericial practicada para acreditar el volcado de archivos desde los ordenadores portátiles de los querellados a dispositivos USB, si bien es cierto que el informe encargado por la querellante deduce que ha existido, no lo es menos que los discos duros de aquellos ordenadores sufrieron diversas manipulaciones por parte de la empresa querellante hasta el momento en que fueron depositados ante un fedatario público para ser entregados al perito (...), sin que haya constancia de que se haya mantenido la cadena de custodia de los mismos (...), de modo que la capacidad de aquel informe para acreditar hechos adversos a los querellados debe ser relativizada, como hace la resolución recurrida*", confirmándose el archivo provisional decretado por el Juzgado de Instrucción.

de la actividad jurisdiccional, encomendando su práctica al Cuerpo técnico policial oportuno. No obstante, esta práctica pese a otorgar mayores garantías al proceso, encontrará normalmente dificultades por parte del órgano policial comisionado al efecto, que ya de por sí suele contar con efectivos personales y materiales manifiestamente insuficientes para acometer las investigaciones policiales acordadas de oficio, repercutiendo negativamente en la dilación o retardo que habrá de sufrir el procedimiento mientras se está a la espera de la recepción del respectivo contraanálisis pericial.

En cuanto al segundo de los problemas antes esbozados con los que puede encontrarse la pericial informática de parte, baste simplemente referir que este tipo de pericias a menudo han de incidir en el análisis y observación de datos de carácter personal, vinculados a la esfera de intimidad de la persona, o bien atinentes al contenido de sus comunicaciones, pudiendo verse afectados derechos fundamentales reconocidos en el art. 18.1, 3 y 4 de la CE. La consecuencia de tal vulneración será la nulidad radical de dicha pericia.

5. VALORACIÓN DE LA PRUEBA INFORMÁTICA.

5.1 Valoración de la prueba documental informática.

En la valoración de las pruebas informáticas rige el art. 741 LECrim relativo a la "íntima convicción o apreciación en conciencia".

Los datos informáticos contenidos en archivos de datos o registrados de flujos de datos exigen por lo general precauciones y medidas especiales para que puedan servir de prueba ante los tribunales. El documento electrónico, entendido como "toda representación en forma electrónica de hechos jurídicamente relevantes, susceptibles de ser presentados en forma humanamente comprensible"[643], es decir, *el conjunto de datos*

[643] Así lo recoge ALVÁREZ CIENFUEGOS-SUAREZ, J.M.: "Los delitos de falsedad y los documentos generados electrónicamente. Concepto procesal y material de documento: nuevas técnicas". Cuadernos de Derecho Judicial, C.G.P.J., Madrid, 1993, pág. 8.

electrónicos que representan los actos y negocios jurídicos, legibles mediante los correspondientes programas o sistemas lógicos y contenidos en discos o soportes magnéticos u ópticos que los almacenan[644], constituye prueba válida en un proceso penal.

La LECrim carece de una regulación expresa del documento electrónico, pero en el proceso penal la admisión del mismo no presenta especiales dificultades en una interpretación actualizada del contenido del art. 726 LECrim, conforme al cual *el Tribunal examinará por sí mismo los libros, documentos, papeles y demás piezas de convicción que puedan contribuir al esclarecimiento de los hechos o a la más segura investigación de la verdad*, adaptando la práctica de tal prueba a sus peculiaridades técnicas, pudiendo en consecuencia, si se considera como auténtico, ser valorado como prueba de cargo o de descargo, surtiendo plenos efectos.

Tales términos son aplicables tanto a los documentos electrónicos en los que se muestran las páginas web, los sms o incluso los e-mails, como la posibilidad de examinar los datos en su formato original, lo cual puede consecuentemente traer los inconvenientes de temporalidad e inaccesibilidad de los llamados documentos virtuales.

Respecto a la valoración del documento, supletoriamente son aplicables los artículos de la LEC, de tal modo que en caso de documentos públicos:

-Nacionales: son de aplicación los arts. 318 a 322 LEC, de los que resulta su plena fuerza probatoria. Es el caso de los documentos notariales, judiciales y administrativos u oficiales.

Tendrán la consideración de documental pública cuando, con las debidas garantías de autenticidad, el contenido y los datos de tráfico se trasvasan a un soporte inteligible bajo la supervisión del LAJ (generalmente en CD) con la misma información sustancial que en el soporte original y, en cualquier caso, indicando los datos suficientes para permitir en su caso su lectura, contradicción y la discusión sobre su veracidad, fiabilidad y autenticidad por las partes afectadas que nieguen dicho material en la vista oral.

[644] ROVIRA DEL CANTO, E**.:** "Tratamiento penal sustantivo de (...)". ob. cit. págs. 477 y 478.

-Documentos públicos extranjeros (art. 323 LEC): harán prueba plena, en los términos del art. 319 de la LEC, cuando así se prevea en tratado, convenio o ley especial.

Y si son documentos privados, se aplica el art. 326 LEC, de manera que si no es impugnado hará prueba plena en los términos del art. 319 de la LEC (incluso copias); si lo es, se valorará conjuntamente con el resto de la prueba, sin perjuicio de que la parte a quien se le haya impugnado un documento pueda proponer prueba acerca de su autenticidad. Es decir que la documental privada, ante la inexistencia de intervención de fedatario público en su adquisición, el mero texto y datos deberán ser adverados por quien los haya conseguido, que deberá, caso de duda o negación, declarar contradictoriamente sobre este extremo en el acto de la vista oral, convirtiendo la prueba en una mezcla de documental y testifical.

En cuanto a los requisitos que debe reunir la copia del documento para ser valorada como prueba de cargo, requiere que se garantice que la información contenida en la copia es la misma que en el original, exprese los datos necesarios para permitir su lectura y ser sometidos a contradicción acerca de su veracidad y autenticidad por las partes que la nieguen[645].

[645] Un caso interesante reflejado en la jurisprudencia viene constituido por la Sentencia de la Sala de lo Penal de la Audiencia Nacional, (Sección 2ª), 31/2009 de 30 de abril. ("caso Tigris", sobre terrorismo islamista). La sentencia, en su [FJ 3°], analiza como cuestión previa a la valoración de la prueba practicada en el juicio la impugnación por parte de las defensas de la intervención de las cuentas de correo electrónico, datos correspondientes a ellas y tráfico de mensajes entrantes y salientes, cuya incorporación al Sumario tiene lugar durante la instrucción judicial como consecuencia de una Comisión Rogatoria librada a las autoridades de Estados Unidos, y que había sido cumplimentada, sin contar con el preceptivo auto judicial autorizante de dicha intervención, previa ponderación de los derechos fundamentales en juego. La contestación a la Comisión Rogatoria librada por el Juzgado Central de Instrucción recoge la información requerida sobre diez cuentas de correo electrónico vinculadas a los acusados en un CD Rom que se adjunta como anexo a la misma, el cual es posteriormente remitido por el Juzgado a un funcionario policial para elaborar un informe técnico sobre el contenido de dicho soporte informático, al ser el mismo inaccesible por encontrarse en un lenguaje informático ilegible sin previa conversión a los lenguajes de uso ordinario. El oportuno informe policial realizado bajo el mandato judicial es aportado a la causa casi 22 meses después de la orden del Juzgado, bajo el título "*Informe sobre las cuentas de correo investigadas en la Operación Tigris*," haciéndose referencia en el mismo a que fue necesario llevar a cabo un procedimiento técnico especializado de conversión a lenguaje legible para llevar a cabo el volcado del contenido del CD Rom. Sobre este particular, razona el Tribunal que *"De la simple lectura de dicho informe se aprecia que no contiene un volcado o trascripción literal en formato legible de la información contenida en el soporte informático, sino información elaborada a partir de su contenido, consistente, según parece, en la trascripción traducida al español del texto de los mensajes asociados a unas determinadas cuentas de correo. Consta, por tanto, en todos los casos únicamente un texto en español, es decir, sin que aparezca el texto original de los mensajes (por el Instructor y el Secretario de manifiesto que algunos mensajes estaban originariamente escritos no solo en lengua árabe sino que también en grafía árabe y otros en lengua árabe pero en grafía latina), sin*

Las copias, si son impugnadas, pueden ser cotejadas por el LAJ u objeto de pericial. En caso de impugnación se exige la presencia de los autores para contradicción, ya que la pericial normalmente sirve más para descartar autoría dudosa que para determinar el autor.

No debe olvidarse que los textos escritos trasmitidos electrónicamente generan mayores dificultades que los manuscritos a la hora de atribuir la autoría o participación en la elaboración o imputación de sus mensajes, pues la información técnica asociada a ellos no siempre la determinan, ya que, como es notorio, se pueden emitir desde un terminal del que el usuario no sea titular, o lo sea compartidamente con otros, obligando a complementar la prueba sobre su autor, no siendo por ello suficiente con conocer el usuario que se asocia a la IP de procedencia -que puede ser dinámica o estar desubicada o simplemente intermediada o anonimizada.

Respecto a la impresión de la pantalla de un móvil, ordenador, correo electónico, mensaje etc., ha declarado de forma reiterada el Tribunal Supremo[646] (en relación por ejemplo, con las transcripciones de diálogos o conversaciones mantenidas por teléfono) que por más que consten en un soporte escrito o incluso sonoro, la prueba de una comunicación bidireccional mediante cualquiera de los múltiples sistemas de mensajería instantánea debe ser abordada con todas las cautelas. La posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio

---

indicación tampoco del idioma original en el que fueron escritos, ni en muchos casos, tampoco, ni siquiera su fecha y hora. En el informe no se hace constar como se llevó a cabo la traducción ni si se contienen la totalidad de los mensajes ni otros pormenores relativos a su elaboración. Este informe aparece simplemente unido a las actuaciones, pero no ha sido objeto de ratificación judicial expresa. Su *autor no ha sido citado a juicio, ni por tanto ha comparecido al acto de la vista, ni como testigo ni como perito".*
Justifica la Sala que no se hace este planteamiento desde una posición puramente formalista: "*Al respecto resulta útil dejar constancia de ciertas importantes dudas que le han surgido en las mínimas comprobaciones que ha tenido ocasión de efectuar sobre el contenido del CD-Rom. Así, ha encontrado, hasta donde le ha sido posible llegar dadas las limitaciones que se han referido con anterioridad, que existiría una aparente falta de correspondencia entre lo por ella misma observado sobre el contenido del CD-Rom, con el contenido que se afirma tiene y aparece impreso a folio 12.624 de las actuaciones, en el 'Informe sobre las cuentas de correo electrónico investigadas en la operacion tigris," ya que todas las carpetas conteniendo los archivos están fechadas 22/05/2006, es decir con fecha muy posterior a la cumplimentación de la Comisión rogatoria por parte de las autoridades competentes".*

[646] SSTS 300/2015, de 19 de mayo, 956/2013 de 17 diciembre, 1024/2007, de 30 de noviembre, 1157/2000, 18 de julio. "*Los denominados "pantallazos" obtenidos a partir del teléfono móvil de la víctima, no son propiamente documentos a efectos casacionales. Se trata de una prueba personal que ha sido documentada a posteriori para su incorporación a la causa. Y aquéllas no adquieren de forma sobrevenida el carácter de documento para respaldar una impugnación casacional".*

de ideas, forma parte de la realidad de las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo. De ahí que la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria. Será indispensable en tal caso la práctica de una prueba pericial[647] que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido (STS 300/2015, de 19 de mayo [FJ 4º].

El correo electrónico se considera, a efectos procesales, como un "documento privado", de lo que se deriva lo siguiente: si la parte que se pueda ver perjudicada por su contenido no los impugna, los correos electrónicos "*harán prueba plena"* en el proceso, en los términos del artículo 319 de la LEC al cual se remite el artículo 326 de la misma norma procesal[648]. Si hay una impugnación de la su autenticidad, deberá practicarse la prueba que resulte pertinente para determinarla y, en función del resultado, el juez *"valorará en íntima convicción y en conciencia"* el correo en cuestión, salvo que quede acreditado que dicho correo era falso, en cuyo caso carecerá de valor probatorio alguno[649]. Y además, para completar el régimen del artículo 326 de la LEC, debe

[647] *Vid.* STS (sala de lo Militar) de 25 de noviembre de 2015, que anula la Sentencia del TMT 1º y devuelve las actuaciones a dicho Tribunal para la práctica de la prueba pericial informática que había sido propuesta por la defensa en tiempo y forma y admitida con el carácter de anticipada respecto de la celebración de la vista del juicio oral con objeto de acreditar la posible manipulación de los SMS en el formato papel en que fueron aportados. "*Para la realización lógica de una pericia tendente a acreditar la posible manipulación de los mensajes obrantes en soporte papel reiteradamente cuestionados, era preciso el cotejo con los soportes originales, sobre todo del teléfono portátil o móvil desde los que se volcaron al papel, o bien eventualmente con otros archivos en que pudieran conservarse dichos mensajes originales".*

[648] NIEVA FENOLL, J. "Práctica y valoración de la prueba documental multimedia". Actualidad civil nº 17. Ed. Wolter kluver. 2009. Pág. 3 "*Todo documento, tambien el multimedia, es auténtico si las partes no lo impugnan, como recuerda claramente el art. 427 LEC".*

[649] VALMAÑA CABANES, A. "La validez probatoria de los correos electrónicos: lo escrito, escrito está". www.Legaltoday.com. Práctica jurídica. *"Puede resultar interesante preguntarse antes que nada qué acredita un correo electrónico cuando el mismo se considera auténtico. Recurriendo al lenguaje un tanto rocambolesco que solemos utilizar los juristas, podríamos decir algo así: un correo electrónico prueba que un determinado mensaje se ha enviado desde una determinada cuenta emisora a una determinada cuenta receptora. ¿Nos garantiza esto que una persona ha enviado un correo a otra? No necesariamente: si pensamos en un ordenador situado en una oficina abarrotada de personas, no resulta imposible que un compañero de trabajo envíe un mail desde la cuenta de otro. De ahí que el juez, incluso cuando el correo es auténtico y un perito ha demostrado que, efectivamente, se transmitió de una cuenta a otra, deba aplicar las reglas de la sana crítica en lugar de considerarlo prueba plena, que es lo que ocurriría si ese supuesto emisor o receptor del mensaje lo hubiera reconocido ya de entrada como*

precisarse que, aunque no se haya propuesto prueba respecto a su autenticidad y aun habiéndose impugnado el documento, éste podrá ser valorado por el juez conforme a las reglas generales.

El juez deberá tener en cuenta circunstancias adicionales al mero envío del mensaje para considerar que representa una auténtica prueba de los hechos discutidos. Será necesario analizar si el ordenador/dispositivo desde el que se ha enviado es de uso privado o pueden acceder terceros, si estaba en casa o en la oficina o en un cibercafé, si tenía claves de acceso o no las tenía, si se ha enviado desde un ordenador o desde un dispositivo móvil... y cualquier otro elemento que pueda tener relevancia a la hora de considerar que una determinada persona ha sido, ciertamente, emisora o receptora de un determinado mensaje y que éste tiene el contenido que se ha sometido a su consideración, además de haberse remitido en la fecha consignada en el mismo.

Quien quiera utilizar esos mensajes como prueba en un juicio debe tomar, por sí mismo, las medidas más oportunas para dotarlos de la eficacia probatoria pretendida[650]. Si se limita a aportar una impresión en papel del correo, poca eficacia podrá obtener si la otra parte lo impugna diciendo, por ejemplo, que el contenido de esa impresión -fácilmente manipulable- no corresponde con el correo adicional[651]. Por ello, es muy conveniente aportar pruebas sobre la autenticidad del correo[652].

---

auténtico. Dicho llanamente, Juan y juan@correo.com son dos realidades distintas y autónomas que tanto pueden haber coincidido en el tiempo y en el espacio de envío de un correo como no."

[650] Es habitual acudir a Notarios para que den fe del contenido del mensaje mediante acta notarial en la que hacen constar el número de teléfonos o dirección de correo, la tarjeta SIM, el IMEI del dispositivo, fecha y hora y el texto del mensaje.

[651] NIEVA FENOLL, J. "Práctica y valoración de la prueba documental multimedia". ob. cit. pág. 9 y 10. "*A efectos probatorios sería muy interesante poder disponer de esos contenidos, que a la vez identifican a sus autores, salvo que haya existido un fallo en la custodia del usuario con respecto a sus contraseñas. Disponer del contenido es sencillo, porque basta con que el usuario entre en su cuenta de correo y haga una copia del mail, en papel o en documento multimedia. Pero lo interesante no es eso -que por otra parte será lo más habitual-, sino que lo relevante habría de ser que la compañía prestadora del servicio, además de los datos técnicos del correo antes referidos, certificara también el contenido a petición del usuario".*

[652] VALMAÑA CABANES, A. "La validez probatoria de los correos electrónicos: lo escrito, escrito está". www. legaltoday.com. Práctica jurídica.
"Existen empresas operadoras que certifican el contenido del mensaje, el momento exacto de su envío, la cuenta del emisor y la cuenta del receptor. Lo hacen valiéndose, además, de códigos alfanuméricos que acreditan -para los ojos expertos- que toda esa información certificada es veraz. Cabe también la posibilidad de aportar al juicio un peritaje informático que acredite ya de entrada la autenticidad de los correos electrónicos, a fin de disuadir a la otra parte de una eventual impugnación y, con ello, facilitar ese

En definitiva, ninguna de estas prevenciones conseguirá probar de forma indubitada que verdaderamente fue una determinada persona quien escribió o recibió el correo pero, sumadas a las circunstancias antes expuestas, harán que resulte muy razonable pensar que sí lo hizo o que sea más verosímil pensar que no fue así[653].

En la jurisprudencia española encontramos sentencias que admiten como prueba la mensajería instantánea a través de aplicaciones como WhastApp o Facebook, como en la SAP de Alicante 4/2014, de 9 de enero, en el ámbito civil, o la SAP de Madrid 533/2014, de 24 de julio y la SAP de Valladolid 119/2015, de 13 de abril, en el ámbito penal. También ha sido rechazada, como en la SAP de Barcelona 109/2016, de 28 de enero, que dice textualmente "*negado por el acusado no sólo la remisión de los mensajes, sino la creación de perfiles en Facebook y no habiéndose aportado otros elementos probatorios para determinar el IP del ordenador desde el que se remitieron los mensajes, ni el número de teléfono al que estaba asociada la línea utilizada o lo que es lo mismo el verdadero origen de las comunicaciones e identidad del remitente, sólo podemos concluir que no se ha practicado prueba suficiente para desvirtuar la presunción de inocencia del acusado y para concluir con rotundidad que remitió mensajes a través de Facebook.* También la SAP de Madrid 51/2013 de 23 de septiembre, que entiende según transcripción textual "*no existe ningún otro medio de prueba que avale su declaración, pues no colma el mismo la prueba documental consistente en las copias de mensajes, conteniendo fotografías, cuyos contenidos no han sido reconocidos por el acusado, ni se ha practicado sobre los mismos prueba pericial informática que acredite su autenticidad y su envío"*. Ello quiere decir que si la otra parte no reconoce el envío de los mensajes se deberá presentar un peritaje informático

efecto de *"prueba plena"* que resulta tan deseable conseguir. Y no está de más tampoco contar con la presencia de un notario que levante acta del modo en que se trata toda aquella información y que refleje que, efectivamente, aquel correo está en aquella bandeja de entrada (realidad expresada, eso sí, con todas las prevenciones que el lenguaje notarial acostumbra a utilizar). Pero lo único que probaría el acta notarial sería la existencia de unos correos en una bandeja de entrada o en una determinada carpeta electrónica y, a lo sumo, podría dejar constancia de la fecha en que -según se viera en el ordenador- podrían haber sido enviados o recibidos".

[653] VALMAÑA CABANES, A. "La validez probatoria de los correos electrónicos: lo escrito, escrito está". Legaltoday.com. Práctica jurídica. "*Tal vez la declaración de testigos o, mejor aún, una grabación en vídeo que acreditase esa autoría del correo sería el modo más óptimo de ir sumando visos de autenticidad al correo electrónico aportado, aunque no siempre será fácil contar con este tipo de pruebas adicionales sobre la prueba electrónica. Se tratará de saber si, con todo ello, se puede ir acercando a Juan y a juan@correo.com hasta dejar claro que coincidieron a la hora de enviar o recibir el correo o que, aplicando las reglas de la sana crítica, resulte la opción más plausible"*.

que avale la autenticidad de los mismos. Además, según la STS 300/2015 en general, para la admisión como prueba de cualquier conversación mantenida a través de una red social, es necesaria la presentación de un informe pericial informático por parte de un perito informático[654].

Respecto a la redes sociales se diferencian dos problemas:

1) Cómo probar el contenido en sí mismo de lo colgado en internet mediante una red social. En principio vale cualquier testigo que lo haya observado directamente, como un agente policial o el denunciante, que tendrá que ratificarlo en el juicio[655].

2) Cómo averiguar el autor concreto del delito: aquí es necesario averiguar la IP que puede ser rastreada policialmente. Pero para averiguar la titularidad de dicha IP se precisará auto judicial motivado, so pena de violación del art. 18 CE. Quien responde a quien pertenece esa IP son precisamente las operadoras[656].

Ahora bien, los datos asociados a la IP que facilitan las operadores tampoco son decisivos para la determinación de la autoría concreta del real infractor (piénsese en los supuestos del uso de técnicas de ingeniería social o informática anonimizadoras y, en su caso, en los supuestos de uso compartido del ordenador). Por ello, no es diferente en este sentido la valoración de la prueba en el ciberdelito que en el delito tradicional, pudiendo utilizarse cualesquiera medios de prueba legalmente admitidos, sea los que aporta la propia técnica, mediante la oportuna prueba pericial informática, cabe la determinación de la convicción judicial por la testifical (uso del ordenador por el inculpado en exclusiva, utilización de apodos, seudónimos o *nicks* etc.) por la confesión

[654] DELGADO MARTÍN, J. "La prueba del whatsapp". ob. cit. pág. 5.

[655] SAN 23/2015, de 30 de septiembre. "(…)*había colgado en su perfil de Facebook la expresión "casado", la cual, como se ha dicho, al igual que otras análogas, como "boda" o "casamiento", es indicativa del propósito inminente de llevar a cabo un atentado de tipo yihadista"*.
SAN 2/2012, de 17 de enero. Enaltecimiento del terrorismo en la red social Tuenti denunciado por la propia empresa.
STS 106/2015, de 19 de febrero, que confirma la condena impuesta por la AN por un delito de enaltecimiento del terrorismo consistente en difundir canciones en internet a través de la red social youtube de una gran difusión, en las que se contenían estrofas claramente laudatorias para condenados por terrorismo o a sus acciones, y, asimismo en clave retórica se citaba a personas u organismos concretos como merecedoras de ser atacadas

[656] FRAGO AMADA, J. A. "La prueba en los delitos cometidos a través de redes sociales. www.legaltoday.com, práctica jurídica. 23 de mayo de 2012.

del inculpado e incluso por determinación indiciaria siempre que convincentemente se razone (analizando a quién le llega el dinero, quién tiene un móvil espurio, a quién le beneficia, los conocimientos informáticos del inculpado, demostrando la mentira de la declaración del imputado, probando que no es posible la infiltración en el uso del ordenador por terceras personas, no dando el acusado explicación). En definitiva, todo lo que permita, mediante el análisis de todos los datos y cualquier otro indicio, llegar a asociar una identidad "virtual" con una identidad real.

5.2 Valoración de la prueba pericial informática.

En lo que respecta a la valoración judicial de la pericia, hay que recordar que pese a su enorme importancia en los ciberdelitos, la prueba pericial, al igual que los restantes medios probatorios regulados en la LECrim, no necesariamente es prueba plena, debiendo valorarse en íntima convicción en función de las circunstancias del caso, lo que aleja el papel del Juez del mero automatismo, aun cuando las pericias tengan mucho peso en ocasiones por su valor de convicción en consonancia con el carácter científico de las mismas.

La investigación judicial de la delincuencia vinculada a las nuevas tecnologías, y especialmente a través de internet, se caracteriza desde el punto de vista probatorio porque no suele conseguir demostrar sus diversas modalidades delictivas mediante la confesión y el testimonio de personas, sino por medio de las pericias que analizan los rastros que todo delito deja en la red. Investigando las huellas técnicas que la acción delictiva ha necesitado para desplegarse, la analítica forense pretende identificar, preservar, presentar y analizar las pruebas que legalmente obtiene de entre la información almacenada o transmitida en cualquier dispositivo y que necesariamente ha realizado quien ha cometido el ciberdelito.

Las características que presentan los datos electrónicos, tales como volatilidad, modificabilidad[657], etc...nos advierten sobre la exigente labor que se requiere por parte

[657] De acuerdo con el HB:171 2003 *Guidelines for the Management of IT Evidence*, la evidencia digital es: "cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un

de los especialistas en temas de informática forense, tanto en procedimientos como en técnicas y herramientas tecnológicas para obtener, custodiar, revisar, analizar y presentar la evidencia presente en una escena del delito.

Hay que tener presente que cualquier duda acerca de la fiabilidad del material de prueba determinará por lo general su inadmisibilidad. Dado que los datos electrónicos pueden modificarse fácilmente sin dejar rastros, ello entraña una pesada carga para las autoridades policiales, que deben reunir esas pruebas de acuerdo con procedimientos transparentes y seguros que les permitan establecer su autenticidad. Para verificar la autenticidad, el Juez debe estar en condiciones de examinar la fiabilidad del proceso de copia y registro del material de prueba, partiendo del portador original o del canal original de datos. También debe poder comprobar la validez de:

- el procedimiento de preservación y la seguridad de la propia preservación;

- cualquier análisis de ese material y si el material presentado ante el tribunal es conforme al material incautado y guardado originalmente.

En las pericias informáticas que aquí se tratan, lo anterior se verifica contrastando el resumen digital recogido sobre la prueba original (basado en algoritmos *hash)* con el de la copia sobre la que se va a emitir la pericia. Si coinciden, el material original y del volcado son idénticos, y las conclusiones de la pericia parten sobre el material ocupado, permitiendo una prueba obtenida con toda la fiabilidad.

De lo contrario, la prueba pericial podría conllevar a resultados discutibles y dudosos, con las consiguientes posibles consecuencias en la fase de valoración de la misma y en la convicción judicial.

---

medio informático". En este sentido, la evidencia digital, es un término utilizado de manera amplia para describir "cualquier registro generado por o almacenado en un sistema informático que puede ser utilizado como evidencia en un proceso legal". La evidencia digital es la materia prima para los investigadores donde la tecnología informática es parte fundamental del proceso. Sin embargo y considerando, el ambiente tan cambiante y dinámico de las infraestructuras de computación y comunicaciones, es preciso detallar las características propias de dicha evidencia en este entorno. La evidencia digital posee, entre otros, los siguientes elementos que la hacen un constante desafío para aquellos que la identifican y analizan en la búsqueda de la verdad:
1. Es volátil; se sobrescribe y se destruye con el uso del dispositivo electrónico.
2. Es anónima
3 .Es duplicable
4. Es alterable y modificable; cambia con el tiempo y es fácilmente modificable.
5. Es eliminable: desaparece con facilidad.

Por todo lo anterior, las pericias informáticas tienen la peculiaridad frente a las que versan sobre corporeidades no reproducibles (cadáveres, máquinas, droga, armas, etc.) de que una vez entregada la copia clónica al perito y habiendo quedado el original guardado por el LAJ, no se ven afectadas por las consideraciones sobre la cadena de custodia, pues la reproducción o copia garantiza fielmente que el objeto de la pericia (cuerpo del delito o pieza de convicción) es el mismo que el aprehendido y analizado.

En resumen, según la STS 53/2011, de 10 de febrero sobre los distintos supuestos de pericia, nos encontraríamos con:

-Pericias preconstituidas, tal y como las denomina el Tribunal Constitucional, que remite al art. 726 para su valoración (AATC 337/2005 de 26 de septiembre, 164/1995 de 5 de junio y 393/1990 y SSTC 24/91, de 11 de febrero y 143/2005, de 6 de junio), que comprende pautas de asistencia, informes forenses, tasaciones practicadas por perito judicial, actas policiales, entendiendo por tales aquellas actuaciones policiales objetivas e irrepetibles (STC 303/93, de 25 de octubre recogida del cuerpo, los efectos o los instrumentos del delito, los croquis o fotografías levantados sobre el terreno o la misma comprobación de la alcoholemia). No precisan ratificación si no son impugnados materialmente, no bastando la mera impugnación formal.

Deben considerarse como tales las actas policiales de recogida de discos duros, archivos, etc. así como las diligencias de volcado de datos.

-Periciales documentadas con privilegio jurisprudencial consolidado. El Pleno no jurisdiccional de la Sala Segunda de 21 de mayo de 1999, afirmó la innecesariedad de ratificación del dictamen de los peritos integrados en organismos públicos, salvo que la parte a quien perjudique impugne el dictamen o interese su presencia para someterlos a contradicción en el plenario y lo hiciera en momento procesal oportuno. Es el caso de los informes realizados por los especialistas informáticos de los centros oficiales del Estado, basados en conocimientos especializados, que no precisan de ratificación para ser valorados, salvo en caso de impugnación tempestiva y con contenido material.

-Otras pericias, documentadas o no, sometidas a la necesidad de ratificación en el juicio oral.

Respecto a las exigencias de la impugnación por la defensa, se sigue una tesis laxa aplicable a toda prueba pericial. Basta con que la defensa impugne el resultado de los dictámenes practicados durante la instrucción o manifieste de cualquier modo su discrepancia con dichos análisis, para que el documento pierda su eficacia probatoria y la prueba pericial deba realizarse en el juicio oral, conforme a las reglas generales sobre carga y practica de la prueba en el proceso penal (STS 587/2003, de 16 de abril), por lo que "no cabe imponer a la defensa carga alguna en el sentido de justificar su impugnación del análisis efectuado" y que "el acusado le basta cualquier comportamiento incompatible con la aceptación tácita para que la regla general (comparecencia de los peritos en el Plenario) despliegue toda su eficacia". (STS 1520/2003 de 17 de noviembre y STS 1511/2000 de 7 de marzo).

La diferencia esencial respecto de otras pericias radica en que la emitida por Centros oficiales no precisa, en caso de ausencia absoluta de impugnación, ratificación (entre otras muchas STS 1446/2003, de 5 de noviembre, STS 13/2004 de 16 de enero y STS 480/2009 de 22 de mayo)."

La falta de exhibición en juicio del material o soporte informático para examinar la información y datos sobre los que versó la pericial no priva de validez al informe pericial[658]. La defensa en este caso debe solicitar las comprobaciones oportunas en

[658] Sentencia del Tribunal Supremo 480/09, de 22 de mayo de 2009, sobre el aparato político de ETA-EKIN y otras organizaciones de su entorno [FJ10] aborda la cuestión planteada por parte de las defensas, relativa a que no estuvo a disposición de la Sala enjuiciadora el ordenador que, según las acusaciones, contenía determinada información contable de determinas empresas investigadas y vinculadas a los acusados, pretendiendo las defensas privar de valor y eficacia al informe pericial confeccionado por los peritos miembros de la Agencia Tributaria ante la "inexistencia de dicho ordenador en la causa", y la imposibilidad de verificar su examen en el acto del plenario. El Tribunal Supremo razona sobre la cuestión precisando que "*Respecto de los incidencias producidas en las sesiones del juicio oral en relación al ordenador, al aducirse por la defensa de uno de los procesados que "para el correcto y debido ejercicio del derecho de defensa, resultaba imprescindible que se accediera al mismo para contrastar sus contenidos, para en él realizar los contrastes precisos y desde él realizar la periciales correspondientes, económicas o de otro tipo," debemos destacar, en primer lugar, en relación con el contenido del ordenador mismo que éste por su configuración informática no fue posible ejecutar copia de seguridad en otro ordenador y hubo que trabajar en él directamente, y en segundo lugar la petición de la defensa, conociendo las especiales características del ordenador, suponía una prueba más propia de la fase instructora que como tal, dada la fecha del informe pericia, tuvo tiempo suficiente para haber solicitado, sobre el contenido del ordenador, otra pericia de tipo contable o transcripción de algún particular que le interesara". Argumentando que "En el caso presente no es factible afirmar esa merma del derecho de defensa por cuanto el recurrente no concretó qué extremos o apuntes de la pericia precisaba comprobar con el contenido del ordenador, datos que, se insiste pudo obtenerlos durante la instrucción y además, en el juicio oral, tuvo la ocasión de interrogar a los peritos sobre todo aquello que consideró conveniente a sus intereses sobre el informe pericial y la documentación que se basó," y que "La defensa se limitó a efectuar una petición genérica respecto de la presencia del ordenador sin precisar extremos de su contenido a los fines señalados, lo que impide valorar la exigida necesariedad, sin perjuicio, como ya se*

instrucción o bien pedir una contrapericia, no admitiéndose la alegación en juicio relativa a inexistencia del ordenador en la sala sin concretar extremos que desee comprobar cuando además puede interrogar al perito. La defensa puede proponer una contra pericia o impugnar expresamente la pericial oficial, impugnación que debe hacerse en el escrito de calificación en el que debe proponerse la práctica de la pericial para el juicio oral, a fin de someter al perito al interrogatorio oportuno (STS 88/1995, de 1 de febrero). La presentación en el acto del juicio de contra-pericias complejas no aportadas en instrucción podría obligar a suspender el juicio para que las restantes partes litigantes puedan ilustrarse suficientemente sobre su contenido.

De otra parte, respecto a los informes de inteligencia[659] el Tribunal Supremo se ha inclinado en sus sentencias 710/2007, de 27 de junio, 119/2007 de 16 de febrero, 556/2006 de 31 de mayo y 1029/2005, de 26 de septiembre, por no considerarlos como prueba pericial, precisando que[660]: "*es claro que apreciaciones como la relativa a la adscripción o no de alguien a una determinada organización criminal, o la intervención de un sujeto en una acción delictiva a tenor de ciertos datos, pertenecen al género de las propias del común saber empírico. Salvo, claro está, en aquellos aspectos puntuales cuya fijación pudiera eventualmente reclamar una precisa mediación técnica, como sucede, por ejemplo, cuando se trata de examinar improntas dactilares. Pero ese plus de conocimiento global no determina, por ello solo, un saber cualitativamente distinto, ni especializado en sentido propio. Y, así, seguirá perteneciendo al género de los*

ha indicado, que pudo conocer tales datos o, en su caso, solicitar otra pericial contradictoria, durante la fase de instrucción de la causa," para concluir, en consecuencia, en la inexistencia de indefensión por la falta de examen en el plenario de la pieza de convicción interesada, desestimando el motivo de impugnación planteado por las defensas.

[659] *Vid.* GUERRERO PALOMARES S. "La denominada prueba de inteligencia policial o pericial de inteligencia". Revista Aranzadi de derecho y proceso penal nº 25, 2001.

[660] STS1029/2005, de 26 de septiembre, "*resulta más que problemático que aquí pueda hablarse de pericial en sentido propio. En efecto, no parece discutible que el perito es un auxiliar experto que suministra al juez conocimientos especializados de carácter científico o técnico, de los que él no dispone, y que son necesarios para formar criterio sobre el thema probandum. Así, en el proceso, es pericia la que se emite a partir de saberes que no son jurídicos y que tampoco corresponden al bagaje cultural del ciudadano medio no especialista. Consecuentemente, no pueden darse por supuestos y deben ser aportados al juicio, para que su pertinencia al caso y su concreta relevancia para la decisión sean valorados contradictoriamente (...) Por tanto, el agente policial exclusivamente dedicado a indagar sobre algún sector de la criminalidad, podrá tener sobre él más cantidad de información que el tribunal que enjuicia un caso concreto relacionado con la misma. Pero ese plus de conocimiento global no determina, por ello solo, un saber cualitativamente distinto, ni especializado en sentido propio. Y, así, seguirá perteneciendo al género de los saberes comunes, susceptibles de entrar en el área del enjuiciamiento por el cauce de una prueba testifical apta para ser valorada por el juez o tribunal, directamente y por sí mismo".*

saberes comunes, susceptibles de entrar en el área del enjuiciamiento por el cauce de una prueba testifical, apta para ser valorada por el juez o tribunal, directamente y por sí mismo".

Ahora bien, aun cuando la sentencia 119/2007 niega la condición de prueba pericial a estos informes, sí precisa que: "participan de la naturaleza de la prueba de indicios, en la medida que aportan datos de conocimiento para el Tribunal sobre determinadas personas y actividades. Y esos datos, si son coherentes con el resultado de otros medios de prueba pueden determinar, en conjunción con ellos, la prueba de un hecho, siempre que éste fluya del contenido de todos esos elementos valorados por el órgano sentenciador".

En definitiva, concluye el Tribunal Supremo, se trata de un medio que no está previsto en la Ley, siendo los autores de dichos informes expertos en esta clase de información que auxilian al Tribunal aportando elementos interpretativos sobre datos objetivos que están en la causa, siendo lo importante si las conclusiones que extraen son racionales y pueden ser asumidas por el Tribunal, racionalmente expuestas y de forma contradictoria ante la Sala. Esencial será constatar si las conclusiones obtenidas por los funcionarios actuantes pueden ser asumidas por el Tribunal a la vista de la documental obrante en la causa y del resto de las pruebas practicadas en el plenario, esto es, si se parte de su consideración como testifical donde debe ponerse atención es en el examen de los documentos manejados por los funcionarios policiales[661].

[661] En este aspecto hace particular hincapié el Tribunal Supremo en la sentencia 480/2009 de 22 de mayo, recaída en el caso "EKIN" y literalmente citada en la STS 985/2009, de 13 octubre. "*Estas investigaciones, y sus resultados expuestos en cada proceso por medio de informes escritos y luego trasladados al juicio oral mediante las declaraciones testificales de sus autores, pueden tener valor como prueba de cargo, evidentemente no como manifestación de las opiniones personales de estos testigos, sino por los documentos manejados que constituyen el fundamento de esas opiniones". "Siendo así, decaerá la pretensión impugnatoria de los recurrentes, tanto si se considera centrada en la exclusiva consideración de la prueba (en realidad específica e innominada legalmente, que participa de una naturaleza como de la otra) como pericial, en cuyo caso habría que estar a lo argumentado por la sala de instancia, como, sobre todo, si se parte de su consideración como testifical, como también insinúan los recurrentes, dado que, en tal supuesto, donde hay que poner la atención es en el examen de los documentos manejados por los funcionarios, sobre su aportación, y, a partir de ellos y de los indicios de este modo proporcionados, en la corrección de las inferencias realizadas por el tribunal de instancia (...); a diferencia de lo que ocurriría con otras pruebas periciales que aporten aspectos científicos o técnicos inaprensibles, por puras limitaciones de la inteligencia humana, por los Tribunales, el componente pericial de los informes de inteligencia, exclusivamente limitado al tratamiento, agrupación y análisis de información con arreglo a experiencia, y, lo que es más importante, los juicios de inferencia alcanzados a la luz de todo ello, resultan fiscalizables en todos sus aspectos por la Sala sentenciadora."*

STS 985/2009, de 13 octubre [FJ 5º] este tipo de prueba, se caracteriza por las siguientes notas:

Por lo demás, para la valoración de la pericial informática, rigen las mismas reglas que para la valoración de la prueba pericial en general[662] por lo que habrá que tener en cuenta si es perito de parte o de designación judicial[663] y si está integrado en

---

1º) Se trata de una prueba singular que se utiliza en algunos procesos complejos, en donde son necesarios especiales conocimientos, que no responden a los parámetros habituales de las pruebas periciales más convencionales;
2º) En consecuencia, no responden a un patrón diseñado en la Ley de Enjuiciamiento Criminal, no obstante lo cual, nada impide su utilización en el proceso penal cuando se precisan esos conocimientos, como así lo ha puesto de manifiesto la jurisprudencia reiterada de esta Sala;
3º) En todo caso, la valoración de tales informes es libre, de modo que el Tribunal de instancia puede analizarlos racional y libremente: los informes policiales de inteligencia, aun ratificados por sus autores no resultan en ningún caso vinculantes para el Tribunal y por su naturaleza no podrán ser considerados como documentos a efectos casacionales;
4º) No se trata tampoco de pura prueba documental: no puedan ser invocados como documentos los citados informes periciales, salvo que procedan de organismos oficiales y no hubieran sido impugnados por las partes, y en las circunstancias excepcionales que señala la jurisprudencia de esa Sala para los casos en que se trata de la única prueba sobre un extremo fáctico y haya sido totalmente obviada por el Tribunal sin explicación alguna incorporada al relato de un modo, parcial, mutilado o fragmentario, o bien, cuando siendo varios los informes periciales, resulten totalmente coincidentes y el Tribunal los haya desatendido sin aportar justificación alguna de su proceder;
5º) El Tribunal, en suma, puede apartarse en su valoración de tales informes, y en esta misma sentencia recurrida, se ven supuestos en que así se ha procedido por los jueces "a quibus";
6º) Aunque cuando se trate de una prueba que participa de la naturaleza de pericial y testifical, es, desde luego, más próxima a la pericial, pues los autores del mismo, aportan conocimientos propios y especializados, para la valoración de determinados documentos o estrategias;
7º) Finalmente, podría el Tribunal llegar a esas conclusiones, con la lectura y análisis de tales documentos.

Sentencia del Tribunal Supremo de 19 enero 2007 (RJ 1771/2007) contiene la siguiente afirmación: *"Precisamente por ello (...), concurriendo estas circunstancias, podrá entenderse que los informes mencionados pueden equivaler a una verdadera prueba pericial, siempre y cuando el objeto de la misma, la documentación, haya sido incorporada a los autos, es decir, lo que es objeto de la pericia (documentos incautados) debe estar a disposición de las partes". A la luz de la jurisprudencia que antecede, no puede este Tribunal menos que considerar legítima la pretensión del Ministerio Fiscal de que se procediera a la admisión como tal prueba de inteligencia policial de los diversos informes que han sido emitidos por los agentes investigadores, con el auxilio de funcionarios de la AEAT (pretensión innecesaria por demás en tanto que los informes forman parte de la causa desde el momento de su respectiva incorporación a la misma). Cuestión distinta es la valoración que nos hayan de merecer atendidas, de un lado, la posibilidad de contraste entre las opiniones emitidas por los funcionarios y la documentación utilizada a tal fin, y, de otro, la manera en que aquellos (citados por el Ministerio Fiscal en calidad de testigos) han depuesto en el acto del juicio. Por lo que respecta al contraste, hemos de traer a colación necesariamente lo sucedido con la ordenación de la documentación que, como piezas de convicción, acompañaba a la causa. En opinión de este Tribunal, lejos de adoptarse las medidas necesarias a fin de preparar el juicio oral y, en concreto, la exhibición de aquellos documentos -prácticamente todos-cuya legitimidad, tanto constitucional -por la procedencia de los registros-como ordinaria ha sido cuestionada por todas y cada una de las defensas, se supeditó su orden a la estructura de la propia investigación, dando por buena la forma en que quedaron a disposición de los agentes investigadores y en que estos los devolvieron al instructor. Como resultado de ello, únicamente acudiendo a los informes policiales, y sólo de manera parcial, dado que no siempre se recoge la reseña de documentos -que, como también se dijo, lo es de los considerados relevantes-podía llegar a consultarse -no sin una previa y penosa búsqueda-el documento original".*

[662] *Vid*. NIEVA FENOLL, J. "La valoración de la prueba". Ed. Marcial Pons, Barcelona, 2010. págs. 285 a 307.

organismos públicos, así como su profesionalidad. También se debe valorar la coherencia interna, la razonabilidad y la exposición detallada del dictamen pericial y el seguimiento de parámetros científicos de calidad en su elaboración. Igualmente habrá de tomarse en consideración la contradicción del parecer expresado en el dictamen tanto con otros dictámenes periciales como con el resultado de otras pruebas. Otro aspecto a considerar, según los casos, sería la cualificación del perito (titulación, conocimiento especializado, experiencia), las técnicas utilizadas por el perito y su posible imperfección, la inmediatez temporal y material del perito con la fuente de prueba, la duración de las operaciones periciales, la conguencia o correlación entre las cuestiones propuestas y los términos del dictamen (vicio por exceso, por defecto, por evasividad), los datos y fuentes de conocimiento de que ha dispuesto el perito, los medios técnicos y equipos de análisis utilizados (si son posibles en principio varios la justificación de que el utilizado es el más adecuado), la verificación técnica del correcto funcionamiento del instrumental, la fiabilidad del programa empleado, la coherencia de las conclusiones, etc. Por último, habrá de valorarse la propia la declaración del perito.

5.3 Valor de la prueba irregular y valor de la prueba ilícita.

Ya se ha dicho que la prueba ilícita no supera el juicio de licitud por haberse obtenido con violación de derechos fundamentales. En concreto, respecto a las diligencias de investigación tecnológica éstas son ilícitas si se practican sin contar con autorización judicial, cuando es requerida, salvo los casos de urgencia; cuando se autoriza el uso de estas técnicas para la investigación de delitos que no legitiman su adopción o cuando la autorización judicial no se ajusta a los principios que la

[663] No puede desconocerse que el informe del perito judicial goza *a priori* de algún *plus* sobre el dictamen pericial de parte. En primer lugar, es un tercero ajeno a las partes, sin ningún interés en el asunto, a diferencia del perito de parte respecto del cual, sin dudar de su imparcialidad, no cabe olvidar que siempre existe un control de origen de la parte en cuanto al dictamen. Es decir, que si el resultado del dictamen le es perjudicial, puede optar por no presentarlo hasta disponer de otro que se adecúe más a lo perseguido. Eso no significa que el perito sea parcial, sino que obedece al hecho común de que el objeto de la pericia puede ser apreciado, con toda lealtad, por distintos peritos, y ofrecer en sus dictámenes conclusiones distintas, pues no se trata de ciencias exactas, pero sin descartar tampoco que, con la mejor fe y de manera tal vez inconsciente, el perito de parte pueda tender a enfatizar aquellos aspectos que más benefician a su principal, a la par que soslayar aquéllos que le puedan perjudicar.

fundamentan (especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida).

La jurisprudencia del TS, en relación con la diligencia de intervención de las comunicaciones, entiende que es ilícita cuando las infracciones son de alcance constitucional como son: la ausencia de fundamento bastante de su autorización, la conculcación del principio de proporcionalidad que ha de regir la decisión del Juez, la absoluta ausencia del acuerdo judicial o los defectos trascendentales en el mismo, así como la total omisión de motivación, la absoluta indeterminación de la clase de delito perseguido, de la identificación del sujeto pasivo o de los encargados de ejecutar la diligencia, de los números telefónicos a intervenir o de los límites temporales para la ejecución de la restricción del derecho fundamental y periodicidad de los informes al Juzgado por parte de los ejecutores de la práctica. También tendrán el mismo carácter las graves incorrecciones en la ejecución de lo acordado, que supongan una extralimitación en el quebranto de los derechos del afectado o de terceros, prórrogas temporales o extensiones a otros teléfonos no autorizados expresamente y, en definitiva, cualquier actuación de los investigadores que incumpla lo dispuesto por el Instructor en lo relativo a los límites constitucionalmente protegidos[664].

En estos casos, la prueba será nula por haber sido obtenida con violación del derecho a la intimidad personal del encausado, el secreto de las comunicaciones, la protección de datos o el derecho a la identidad virtual según disponen los arts. 18.1, 18.3 y 18.4 de la Constitución Española (artículo 11.1 de la LOPJ) y carente de toda eficacia probatoria.

Por el contrario, la prueba irregular es la que no supera el juicio de fiabilidad, sea porque existen dudas sobre la autenticidad e integridad de la información o por el modo de obtención de ésta, o porque existen dudas en el contraste con la finalmente aportada en juicio. Cuando según la STS 201/2006, de 1 de marzo, no se transciende de la condición de meras infracciones procesales, otras irregularidades que no afecten al derecho constitucional al secreto de las comunicaciones y que tan sólo privan de la suficiente fiabilidad probatoria a la información obtenida, por no gozar de la necesaria

[664] STS 201/2006, de 1 de marzo [FJ1º] distingue las infracciones de alcance constitucional y de aquellas que no transcienden de la condición de meras infracciones procesales

certeza y de las garantías propias del proceso o por sustraerse a las posibilidades de un pleno ejercicio del derecho de defensa al no ser sometida a la necesaria contradicción[665].

Las consecuencias que se derivan de la conexión con la prueba ilícita y la prueba irregular son diferentes[666].

La prueba ilícita carece totalmente de eficacia probatoria contaminando en el mismo sentido al resto de las pruebas que derivan de ella (doctrina de los frutos del árbol envenenado) siempre que exista una conexión causal con la prueba ilícita, conservando la eficacia probatoria el resto de las pruebas no conexas[667].

En relación a la prueba irregular, no toda irregularidad en la práctica y desarrollo de las diligencias de investigación tecnológica tiene relevancia para motivar su anulación y mucho menos la nulidad de la prueba refleja derivada[668], sino que existen simples irregularidades procesales que agotan su alcance en la imposibilidad de valorar la prueba en sí misma, pero no impiden la valoración de la prueba refleja derivada[669].

---

[665] Como señala la STS 998/2002 de 3 de junio, tales requisitos son los propios que permiten la valoración directa por el Tribunal sentenciador de todo el caudal probatorio y que por ello se refieren al protocolo de incorporación al proceso, y la efectiva disponibilidad de la aportación de las cintas originales integradas al proceso y la efectiva disponibilidad de este material para las partes, junto con la audición o lectura de las mismas en el juicio oral lo que le dota de los principios de oralidad y contradicción; salvo que, dado lo complejo o extenso que pueda ser su audición se renuncie a la misma bien entendido que dicha renuncia no puede ser instrumentalizada por las defensas para tras interesarla, alegar posteriormente vulneración por no esta correctamente introducidas en el Plenario".

[666] MIRANDA ESTRAMPES, M. "La prueba ilícita: la regla de exclusión probatoria y sus excepciones. Revista Catalana de Seguretat Pública. Mayo 2010. pág. 133.
RIVES SEVA. AP. "La prueba en el proceso penal". Ed. Aranzadi, sexta edición, Pamplona, 2016. pág. 148.

[667] RUIZ VADILLO, E. "Estudios de Derecho Procesal Penal". Ed. Comares, Granada, 1995, pág. 48 y ss.

[668] Así, la STS 1220/2011, de 11 de noviembre, frente a una alegación de que no se entregó a la parte copia de las grabaciones con anterioridad al juicio, que no se tradujeron las conversaciones del catalán y que no se informó a los imputados en el momento de la detención de que sus conversaciones habían sido intervenidas, señala que "*las alegaciones de la parte recurrente son más formales que sustantivas, pues ni se aportan datos y argumentos que permitan apreciar una limitación material y efectiva del derecho de defensa con repercusión en el resultado probatorio, ni tampoco en la fase de juicio oral dio muestras la parte de que realmente tuviera interés en valerse del contenido de las conversaciones telefónicas, pues no propuso la escucha de ninguna de las grabaciones ni tampoco formuló protesta por posibles situaciones de indefensión".*

[669] El juicio de fiabilidad sirve para acreditar la "mismidad" del objeto analizado, la correspondencia entre el efecto y el análisis o informe, su autenticidad. No es presupuesto de validez sino de fiabilidad. Cuando se rompe no nos adentramos en el campo de la ilicitud o inutilizabilidad probatoria, sino en el de la menor fiabilidad (menoscabada o incluso aniquilada) por no haberse respetado algunas garantías. Son dos planos

En este sentido, señala la STS 201/2006, de 1 de marzo, que "debemos distinguir en relación a la validez de las pruebas obtenidas de intervenciones telefónicas, aquellas que resultan de infracciones de alcance constitucional en relación al derecho fundamental al secreto de las comunicaciones, que acarrearán, sin duda, la nulidad absoluta de sus resultados como prueba, e incluso la eventual contaminación invalidante de las otras pruebas derivadas directamente de esta irregular fuente principal, a tenor de lo dispuesto en el artículo 11.1 de la LOPJ (STS 999/2004 de 19 de septiembre), de aquellas las infracciones que tuvieren un mero carácter procesal, cuya consecuencia alcanzará tan sólo al valor probatorio de los productos de la interceptación de las comunicaciones, manteniendo aún su valor como instrumento de investigación y fuente de otras pruebas de ella derivadas".

La falta de fiabilidad no constituye, de por sí, vulneración de derecho fundamental alguno[670].

Habrá que alegar la causa que motiva la falta de fiabilidad del material probatorio, como puede ser si se comprueba que no se procedió al correcto sellado y precintado de los elementos probatorios, si se acredita que se ha producido una deficiente custodia policial de dicho material, que no estaba a salvo de eventuales manipulaciones externas, tanto de carácter cuantitativo como cualitativo[671]. Del mismo modo, si se constata la ausencia de control judicial[672] en las medidas adoptadas que vicia la validez de la prueba o los informes periciales efectuados sobre un material

---

distintos. La ilicitud no es subsanable. Otra cosa es que haya pruebas que por su cierta autonomía escapen del efecto contaminador de la vulneración del derecho (desconexión causal o desconexión de antijuricidad). Sin embargo la ausencia de algunas garantías normativas, lo que lleva es a cotejar todo el material probatorio para resolver si han surgido dudas probatorias que siempre han de ser resueltas en favor de la parte pasiva; pero no a descalificar sin más indagaciones ese material probatorio" (STS 777/2013, de 7 de octubre).

[670] El juicio de fiabilida no es un fin en sí mismo, sino que tiene un valor instrumental, lo único que garantiza es la indemnidad de las evidencias desde que son recogidas hasta que son analizadas, lo que en caso de quiebra puede afectar a la credibilidad del análisis pero no a su validez. (STS 795/2014, de 20 de noviembre)

[671] FIGUEROA NAVARRO, C Y DEL AMO RODRÍGUEZ, A. "La cadena de custodia de las pruebas y los protocolos de actuación de la policía científica". Policía Científica. 100 años de ciencia al servicio de la Justicia. Ministerio del Interior. Material de las Jornadas Centenario de la Policía Científica Española, junio 2011. Pág. 325.

[672] STC 121/1998, de 15 de junio, [FJ 3] "*las irregularidades en el control judicial cuando no se realizan en la ejecución del acto de intervención sino al incorporar a las actuaciones sumariales su resultado, no generan lesión del derecho fundamental"* y STC 49/1999, de 5 de abril, [FJ 11].

informático que se incorporó sin que quedara acreditado el cumplimiento de las debidas garantías de custodia policial y control judicial sobre su identidad e integridad.

Sólo en caso de que la sentencia se haya dictado prescindiendo absolutamente del juicio de fiabilidad en los casos en que la falta de fiabilidad vulnera las garantías esenciales del procedimiento, por haber sido objeto de valoración pruebas incorporadas al procedimiento penal sin las debidas garantías, podría prosperar un recurso de amparo por vulneración del derecho a un proceso con todas las garantías[673].

Respecto a la prohibición de valoración de la prueba ilícita, hay que determinar cuál sea la extensión de la prohibición de valoración de este resultado probatorio: si ha de quedar ceñido al contenido fáctico ilícitamente obtenido y a las pruebas que directamente se deriven, o si, por el contrario, ha de extenderse a todas las pruebas que directa o indirectamente tengan como causa aquella prueba de valoración prohibida.

A este respecto, debe tenerse muy en cuenta que una sentencia condenatoria sustentada en escuchas telefónicas vulneradoras del art. 18.3 CE, infringe la *presunción de inocencia* o el derecho *"a un proceso con todas las garantías"* del art. 24.2 CE, ya que una de las garantías de este derecho fundamental consiste en no ser condenado mediante una prueba obtenida con violación de las normas tuteladoras de los derechos fundamentales. La cuestión no es baladí, según GIMENO SENDRA, pues la infracción de la presunción de inocencia es un vicio "*in iudicando*" por lo que el restablecimiento de este derecho fundamental lo efectuará el propio TC mediante la anulación de la Sentencia de instancia, lo que equivaldrá a una Sentencia absolutoria. Pero, si se sostiene la segunda tesis que encierra un vicio "*in procedendo*", dicho restablecimiento no ocasionará la absolución del condenado, sino la nulidad del juicio oral y la retroacción de las actuaciones a fin de que al inicio de las sesiones, en la comparecencia previa del proceso penal abreviado, el tribunal decida admitir otra prueba válida de

[673] STC 41/2003, de 27 de febrero, [FJ 6], o STC 230/2002, de 9 de diciembre, [FJ 9].

cargo propuesta por la acusación, de cuya práctica y valoración dependerá la absolución o condena del acusado[674].

La jurisprudencia de nuestros Tribunales recibió el influjo de las doctrinas norteamericanas de la "*exclusionary rule*" y de la "teoría del fruto del árbol envenenado" (*fruit of the poisonous tree*), doctrinas que el Tribunal Supremo de Estados Unidos hizo derivar de la Cuarta Enmienda a su propia Constitución.

A fin de determinar la extensión de los efectos de la prueba prohibida en la presunción de inocencia, surgieron y coexisten en el derecho comparado dos grandes tesis, la directa y la refleja o doctrina norteamericana del fruto del árbol envenenado, habiéndose inclinado el art. 11.1 de la LOPJ por esta última teoría, al disponer que *no surtirán efecto las pruebas obtenidas directa o indirectamente, violentando los derechos o libertades fundamentales*[675].

La prohibición de valoración de la prueba ilícita y de su efecto reflejo pretende otorgar el máximo de protección a los derechos fundamentales constitucionalmente garantizados y, al mismo tiempo, ejercer un efecto disuasorio de conductas anticonstitucionales en los agentes encargados de la investigación criminal ("*Deterrence effect").*

La prohibición alcanza tanto a la prueba en cuya obtención se haya vulnerado un derecho fundamental como a aquellas otras que, habiéndose obtenido lícitamente, se basan, apoyan o deriven de la anterior, ("directa o indirectamente"), pues sólo de este modo se asegura que la prueba ilícita inicial no surta efecto alguno en el proceso. Prohibir el uso directo de estos medios probatorios y tolerar su aprovechamiento indirecto constituiría una proclamación vacía de contenido efectivo, e incluso una incitación a la utilización de procedimientos inconstitucionales que, indirectamente, surtirían efecto. Los frutos del árbol "envenenado" están (art. 11.1 de la LOPJ), jurídicamente contaminados.

---

[674] GIMENO SENDRA, V. "Derecho Procesal Penal". Lección 22. Ed. Thomsom Reuters. 2ª edición octubre 2015 pág. 16. "*Hasta el año 1999 la jurisprudencia del TC venía subsumiendo el restablecimiento de este derecho a través de la presunción de inocencia. A partir de la STC 49/1999 suele efectuar dicha subsunción dentro del derecho a un proceso con todas las garantías, si bien no faltan fallos que todavía lo incluyen en la presunción de inocencia .*

[675] MIRANDA ESTRAMPES, M. "La prueba ilícita: la regla de exclusión probatoria(…)". ob.cit. pág. 134 y 135.

El efecto expansivo previsto en el art. 11.1 de la L.O.P.J únicamente faculta para valorar pruebas independientes, es decir que no tengan conexión causal con la ilícitamente practicada, debiéndose poner especial atención en no confundir "prueba diferente" (pero derivada), con "prueba independiente" (sin conexión causal)".

Aunque en sus orígenes el Tribunal Constitucional suscribiera la teoría directa, a partir de su sentencia 85/1994, de 14 de marzo, consagró la doctrina de los "frutos del árbol envenenado"[676] y se instauró, por vez primera en nuestro país, la eficacia refleja de la prueba prohibida. Sin embargo, la jurisprudencia posterior del Tribunal Constitucional, a partir del Pleno reflejado en la STC 81/1998, de 2 de abril matizó aquél criterio, al desarrollar la doctrina de "*la conexión de antijuridicidad"*. De esta doctrina constitucional se deduce que el efecto anulatorio no se deriva sin más de la conexión causal o natural entre la prueba ilícita y la prueba derivada, sino de la conexión jurídica entre ambas, o conexión de antijuridicidad, que exige un examen complejo y preciso que va más allá de la mera relación de causalidad natural[677].

Nótese que la declaración contenida en el art. 11.1 LOPJ no vincula al TC y así se encarga de señalarlo la propia STC 85/1994 cuando, en su FJ 4º, afirma que dicho efecto reflejo ha de obtenerse "ahora también *en el plano de la legalidad* en virtud de lo dispuesto en el art. 11.1 de la LOPJ". Por lo demás, el TC ha sido siempre muy cuidadoso en no elevar dicha declaración al rango constitucional, lo que conllevaría la petrificación universal de la doctrina anglosajona de la prueba prohibida[678]. No existe, por tanto, un derecho constitucional a la desestimación de la prueba ilícita (STC 114/1984, de 29 de noviembre [FJ 2º]).

---

[676] El supuesto que motivó aquella sentencia (la STC 85/1994) fue una escucha telefónica ilegal por falta de motivación en la resolución judicial. El Tribunal de instancia había fundamentado su sentencia de condena, tanto en el resultado de la intervención telefónica, como en el acta de aprehensión por la policía de un pequeño alijo de droga que le había sido ocupado a un tercero que actuaba como mensajero entre los traficantes de droga y de cuyo transporte había podido tomar conocimiento la policía mediante la escucha telefónica practicada un día antes. Ante tales antecedentes fácticos el TC declara que "una vez establecido que la intervención del teléfono... vulneró su derecho al secreto de las comunicaciones, reconocido en el art. 18.3 CE, hemos de concluir que *todo elemento probatorio que pretendiera deducirse del contenido de las conversaciones intervenidas no debió ser objeto de valoración probatoria".*

[677] ASENCIO MELLADO, J. M. "Intervención de las comunicaciones y la prueba ilícita". Universidad de Alicante. Mayo de 2011, pág. 41 https://www.unifr.ch/ddp1/derechopenal/articulos/a_20110507_02.pdf

[678] GIMENO SENDRA, V. "Derecho Procesal Penal" Lección 22. ob. cit. pág. 16.

Por ello, ante el peligro de frustración del *ius puniendi* que la indiscriminada aplicación de esta doctrina puede comportar, tanto la doctrina como la jurisprudencia, se han manifestado reacias a la instauración, con carácter universal (esto es, para la valoración de la totalidad de los actos de prueba), de la teoría refleja de la prueba prohibida[679].

Es fácil constatar que en los países de nuestro entorno la eficacia indirecta de la prueba ilícita no se aplica de forma absoluta o ilimitada, sino una forma matizada muy próxima a la doctrina de nuestro Tribunal Constitucional[680].

---

[679] GIMENO SENDRA, V. "Derecho Procesal Penal". ob. cit. pág. 16. Aunque en algunas resoluciones la jurisprudencia del TS haya podido consagrar la teoría de la eficacia indirecta (ATS 18 de junio de 1992 y SSTS 25 de junio de 1993 y 29-6-1993), la doctrina mayoritaria es la inversa, es decir, la de la eficacia directa, de tal suerte que la nulidad de la intervención telefónica no impide la prueba del hecho a través de otro medio probatorio: SSTS 31 de octubre de 1990, 9 de octubre de 1992, 17 de marzo de 1993, 5 de abril de 1993, 30 de abril de 1993, 7 de mayo de 1993, 15 de julio de 1993 y 22 de octubre de 1993.

[680] *Vid*. STS 912/2013 de 4 de diciembre [FJ1º] que hace un estudio comparativo de los distintos sistemas. Así por ejemplo, en Portugal, donde la regla de exclusión de la prueba ilícita está incorporada a la propia *Constitución (art 32*), el denominado " *efeito-a-distancia* ", o efecto reflejo de la nulidad en otras pruebas derivadas, está matizado por la singularidad del caso, el tipo de prohibición de prueba vulnerado, la naturaleza e importancia del derecho en conflicto, el bien jurídico o interés sacrificado, el sujeto pasivo de la vulneración, etc.
En Italia, donde la regla de la "*inutilizzabilitá*" de las pruebas obtenidas quebrantando prohibiciones legales fue incorporada al *art 191 del Códice di Procedura Penale de 1988, la polémica figura de la " inutilizzabilitá derivata* " se aplica también de forma matizada. La ausencia de una normativa específica sobre la propagación de la nulidad, salvo en materia de secreto de Estado (Ley 3 de Agosto de 2007) da lugar a soluciones jurisprudenciales muy variadas. Como ejemplo de exclusión de la ineficacia derivada puede citarse la Sentencia de la Corte de Casación, Cass. Sec.VI, de 27 de marzo de 2009.
Algo similar se aprecia en la práctica procesal francesa con el "principio de lealtad en la aportación de la prueba", en la alemana, en la que se aplica la "teoría de la ponderación de intereses" por la que la vulneración de una prohibición probatoria no conlleva necesariamente la prohibición de utilización de la prueba derivada (" *fernwirkung des Beweisverbots* "), en función de la gravedad del hecho y el peso de la infracción procesal concreta, o en el sistema procesal penal holandés en el que la ilicitud probatoria se introdujo en 1996 en el *art 359 del Código de Procedimiento Procesal* , pero en el que la calificación de una prueba como derivada de otra prueba ilícita no acarrea necesariamente la aplicación de una regla de exclusión, aplicándose los principios de proporcionalidad y subsidiariedad.
Y si acudimos fuera del espacio judicial europeo, al propio Tribunal Supremo norteamericano, pionero en la aplicación de esta doctrina (" *fruits of the poisonous tree*"), es indudable que resoluciones como Hudson vs. Michigan, o Herring vs. United States, han atenuado mucho los efectos de la " *exclusionary rule* ".
En el sistema de justicia de Estados Unidos el verdadero y único fundamento de la "*exclusionary rule*" es disuadir a la policía de llevar a cabo actividades de investigación ilícitas, finalidad más conocida como *deterrent effect*, consagrada en US vs. Calandra (414 US 338, 1974) y US vs. Janis (428 US 433, 1976). Así, en US vs. Janis el Tribunal Supremo norteamericano declaró que "el principal propósito de la exclusión de las pruebas ilícitas, si no el único, es evitar las conductas policiales ilícitas", añadiendo más adelante que "la regla por la que se excluye la prueba obtenida en violación de la IV Enmienda, tiende a garantizar los derechos generalmente reconocidos en dicha Enmienda a través de un efecto disuasorio (de la violación misma) y no tanto como expresión de un derecho constitucional subjetivo de la parte agraviada".

Fruto del alcance restringido de la *exclusionary rule* y de la doctrina de los frutos del árbol envenenado se fueron reconociendo paulatinamente distintas excepciones:

Entre las excepciones se halla la excepción de la buena fe en la actuación policial, cuyo origen se encuentra en el caso *Leon vs. US* (468 US 897, 1984). Dicha excepción, acogida por el Tribunal Constitucional en su STC 22/2003, 10 de febrero se aplica cuando la Policía actúa en la creencia de que su comportamiento se ajusta al ordenamiento jurídico y no viola derecho fundamental alguno. La exclusión de la prueba así obtenida carecería de justificación, pues con ello no se consigue el efecto de prevenir conductas policiales futuras de carácter ilícito (*deterrent effect*).

Otra excepción es la del descubrimiento inevitable (*inevitable discovery*), no cabría la exclusión de la prueba si la misma hubiera sido descubierta inevitablemente por una actuación policial respetuosa con los Derechos Fundamentales, independiente de la inicial ilicitud cometida. Dicha excepción se apreció, como submodalidad de la excepción de la fuente independiente (*hypothetical independent source doctrine*), en el caso *Nix v. Williams* (467 US 431, 1984)[681], siendo acogida por nuestro Tribunal Supremo (STS 974/1997, de 4 de julio [FJ4º]) si bien limitando su aplicación a los supuestos de actuaciones policiales de buena fe.

En definitiva, la aplicación absolutamente ilimitada de la regla de la contaminación de los frutos del árbol prohibido carece en el sistema procesal penal actual de referentes en el Derecho Comparado, por lo que la aplicación de la doctrina matizada del Tribunal Constitucional a través de la teoría de la conexión de antijuridicidad resulta lo más coherente con el modelo procesal penal vigente de los países de nuestro entorno.

[681] Los hechos en *Nix v. Williams* consistieron que en un interrogatorio ilegal, el acusado confesó ser el culpable de un homicidio y llevó a la policía al lugar donde había enterrado a la víctima. El Tribunal excluyó las declaraciones del acusado, sin embargo, no aceptó que el cuerpo de la víctima fuera también excluido como resultado del interrogatorio ilegal ya que el mismo se habría descubierto en cualquier caso durante la búsqueda que estaba teniendo lugar antes de la declaración por más de doscientos voluntarios según un plan de rastreo que incluía la zona donde finalmente se encontró el cadáver. El Tribunal Supremo norteamericano admitió el resultado de la confesión sobre la base de que, aunque ésta no se hubiera producido, el cuerpo de la víctima habría sido inevitablemente encontrado, con tan solo una pocas horas de diferencia, durante la batida policial que estaba teniendo lugar en la zona.

En el momento actual, la construcción del TC, desde la STC 81/1998 hasta esta fecha, descansa sobre la teoría de la "*conexión de antijuricidad*", doctrina que la STC 167/2002, de 18 de septiembre resume con acierto: *"...en aquella Sentencia (la STC 81/1998) el Tribunal Constitucional estableció un criterio básico para determinar cuándo las pruebas derivadas de otras constitucionalmente ilegítimas podían ser valoradas o no, que cifró en determinar si, además de estar conectadas desde una perspectiva natural, entre unas y otras existía lo que denominó conexión de antijuridicidad*. "

Para tratar de determinar si esa conexión de antijuridicidad existe o no, se ha de analizar, en en primer término, y desde una perspectiva interna, la índole y características de la vulneración del derecho constitucional materializadas en la prueba originaria, así como su resultado, con el fin de determinar si, desde un punto de vista interno, su inconstitucionalidad se trasmite o no a la prueba obtenida por derivación de aquélla. También, desde una perspectiva que pudiéramos denominar externa, las necesidades esenciales de tutela que la realidad y efectividad del derecho constitucional exige.

Pero todo ello, teniendo en consideración que estas dos perspectivas son complementarias, pues sólo si la prueba refleja resulta jurídicamente ajena a la vulneración del derecho y la prohibición de valorarla no viene exigida por las necesidades esenciales de tutela del mismo, cabrá entender que su efectiva apreciación es constitucionalmente legítima al no incidir negativamente sobre ninguno de los dos aspectos que configuran el contenido del derecho fundamental sustantivo.

De manera que es posible que la prohibición de valoración de pruebas originales no afecte a las derivadas, si entre ambas, en primer lugar, no existe relación natural o si, en segundo lugar, no se da la conexión de antijuridicidad.

El Tribunal Supremo en Sentencias 320/2011, de 22 de abril, 988/2011, de 30 de septiembre y 811/2012, de 30 de octubre efectúa un resumen del estado de la cuestión

en la jurisprudencia de la Sala Segunda y asume la doctrina del Tribunal Constitucional[682].

Así, sostiene que la conexión de antijuridicidad, también denominada *prohibición de valoración*, supone el establecimiento o determinación de un enlace jurídico entre una prueba y otra, de tal manera que, declarada la nulidad de la primera, se produce en la segunda una conexión que impide que pueda ser tenida en consideración por el Tribunal sentenciador a los efectos de enervar la presunción de inocencia del acusado.

[682] STS 912/2013 de 4 de diciembre [FJ 1º] "*Para tratar de determinar si esa conexión de antijuridicidad existe o no, hemos de analizar, según el Tribunal Constitucional cuya doctrina en esta materia nos vincula (art 5 1º LOPJ) , en primer término la índole y características de la vulneración del derecho al secreto de las comunicaciones materializadas en la prueba originaria, así como su resultado, con el fin de determinar si, desde un punto de vista interno , su inconstitucionalidad se transmite o no a la prueba obtenida por derivación de aquélla; pero, también hemos de considerar, desde una perspectiva que pudiéramos denominar externa , las necesidades esenciales de tutela que la realidad y efectividad del derecho al secreto de las comunicaciones exige. Estas dos perspectivas son complementarias , pues sólo si la prueba refleja resulta jurídicamente ajena a la vulneración del derecho y la prohibición de valorarla no viene exigida por las necesidades esenciales de tutela del mismo, cabrá entender que su efectiva apreciación es constitucionalmente legítima, al no incidir negativamente sobre ninguno de los aspectos que configuran el contenido del derecho fundamental sustantivo (STC 81/98).Y desde esta resolución (STC 81/98) conviene destacar que el Tribunal Constitucional considera que cuando, desde la perspectiva interna , la infracción constitucional radica en la falta de expresión parcial del presupuesto legitimador de la injerencia en el derecho fundamental, y en consecuencia no consta que dicho presupuesto no concurriese íntegramente en la realidad y, por lo tanto, que la injerencia no hubiese podido llevarse a cabo respetando todas las exigencias constitucionales inherentes a la intervención de las comunicaciones telefónicas, la valoración de la prueba refleja practicada no vulnera el derecho a un proceso con todas las garantías si se aprecia la concurrencia de un supuesto de ruptura de la conexión de antijuridicidad (en el caso enjuiciado por el Tribunal Constitucional, el descubrimiento inevitable, es decir que la ocupación de la droga se hubiera obtenido, también, razonablemente, sin la vulneración del derecho). Al mismo tiempo, desde la perspectiva externa, aunque la necesidad de tutela del derecho fundamental al secreto de las comunicaciones telefónicas es especialmente intensa, de lo expuesto en la STC 81/98 se desprende que, cuando no nos encontremos ante una injerencia llevada a cabo sin intervención judicial, ni ante una intervención acordada por resolución absolutamente inmotivada, sino ante una resolución judicial en que la expresión de sus fundamentos justificativos haya sido declarada insuficiente, la necesidad de tutela inherente al derecho al secreto de las comunicaciones puede quedar satisfecha sin que resulte necesario extender dicha prohibición a las pruebas derivadas . En consecuencia, como las dos perspectivas son complementarias, aunque la prohibición de valorar la prueba refleja no venga exigida en estos casos de insuficiencia de motivación de la resolución judicial por las necesidades esenciales de tutela del derecho fundamental, si es necesario que la prueba refleja resulte jurídicamente ajena a la vulneración del derecho y en consecuencia que se aprecie alguna causa jurídica de desconexión (descubrimiento inevitable, vínculo atenuado, hallazgo casual, fuente independiente, ponderación de intereses, etc.)" De conformidad con esta doctrina, habrá el juzgador de examinar con atención la relación de causalidad existente entre el resultado probatorio inconstitucionalmente obtenido y el de los demás medios de prueba, de tal suerte que, para extender su conocimiento a esos otros medios de prueba, habrá de comprobar la ausencia de dicha relación de causalidad o de antijuricidad o, dicho en otras palabras, tendrá que acreditarse que el hecho punible se habría probado, en cualquier caso, con independencia de la prueba ilícita obtenida con infracción de la Constitución.*

La prohibición de valoración se encuentra anclada constitucionalmente en el derecho a un proceso con todas las garantías, que impide la utilización de un medio probatorio en cuya obtención se haya producido una vulneración de derechos constitucionales, y su concreción legal se establece en el art. 11.1 -inciso segundo- de la LOPJ.

Ahora bien el efecto directo y el indirecto, tienen significación jurídica diferente. En principio, no podrán ser valoradas -si se quiere, no surtirán efecto, en la terminología legal- aquellas pruebas cuyo contenido derive directamente de la violación constitucional. Por ejemplo, en el caso de que se declare la infracción del derecho al secreto de las comunicaciones, directamente no es valorable el contenido de tales escuchas, es decir, las propias conversaciones que se hayan captado mediante algún procedimiento de interceptación inconstitucional. En el supuesto de que lo conculcado sea la inviolabilidad del domicilio, no podrá ser valorado el hallazgo mismo obtenido por tal espuria fuente.

La significación de la prohibición de su obtención indirecta es más complicada de establecer, y ha de ser referida a las pruebas obtenidas mediante la utilización de fuentes de información procedentes de pruebas ilícitas, siempre que exista entre ellas una conexión de antijuridicidad, es decir que no concurran supuestos de desconexión como el hallazgo casual, el descubrimiento inevitable o la flagrancia delictiva, entre otros.

La importante Sentencia 81/1988, de 2 de abril, dictada por el Pleno del Tribunal Constitucional, estableció que las pruebas reflejas son, desde un punto de vista intrínseco, constitucionalmente legítimas. Por ello, para concluir que la prohibición de valoración se extiende también a ellas, habrá de precisarse que se hallan vinculadas a las que vulneraron el derecho fundamental sustantivo de modo directo, esto es, habrá que establecer un nexo entre unas y otras que permita afirmar que la ilegitimidad constitucional de las primeras se extiende también a las segundas (conexión de antijuridicidad). En la presencia o ausencia de esa conexión reside, pues, la ratio de la interdicción de valoración de las pruebas obtenidas a partir del conocimiento derivado de otras que vulneran el derecho al secreto de las comunicaciones.

En cuanto a su naturaleza, la conexión entre unas y otras pruebas, es un juicio de experiencia acerca del grado de conexión que determina la pertinencia o impertinencia de la prueba cuestionada.

El mecanismo de conexión/desconexión se corresponde a un control, al que ha de proceder el órgano judicial que ha de valorar el conjunto del material probatorio en el proceso penal de referencia.

De dicha doctrina se infiere que si el Tribunal hubiera de fundar su convicción sobre otras pruebas, distintas de la que trae causa de su ilicitud, habrá de plasmar en la Sentencia el juicio de desconexión de dichas pruebas con respecto a la inconstitucional (STC 259/2005 de 24 de octubre)[683]. Dicha conexión de antijuricidad sucede mediante la confesión ante la autoridad judicial libremente manifestada, no obstante la inconstitucionalidad de la intervención telefónica (SSTS 650/2016, de 15 de julio, 654/2012, de 20 de julio, 821/2012, de 31 de octubre); pero si dicha confesión es prestada mediante coacciones, ausencia de información de los derechos o sin asistencia de abogado, tampoco puede el Tribunal fundar en ella una Sentencia de condena (STS 301/2013, de 18 de abril, 2/2011, de 15 de febrero).

[683] SAP de Valencia (sección 2ª) 254/2013 de 25 marzo (testifical desvinculada del registro nulo). SAP de Huelva (sección 3ª) 48/2014, de 20 de febrero (conexión de antijuricidad).

CONCLUSIONES

PRIMERA.- Internet ha influido significativamente en la actividad criminal al generar nuevas formas de criminalidad y servir como instrumento para la comisión de otros delitos tradicionales. Por ello, la investigación del denominado ciberdelito exige conocer las características técnicas básicas de internet (red mundial con conexiones instantáneas y con una estructura en red descentralizada que se basa en la representación digital de la información y permite las conexiones en tiempo real entre las personas, independientemente de su ubicación).

SEGUNDA.- Por ciberdelito cabe entender todas las conductas sancionadas por el Código Penal y las posibles conductas aún no tipificadas pero que pudieran serlo, que tengan vinculación con la informática y las redes, bien en su medio comisivo, bien en el objeto sobre el que recae la conducta, bien en ambos. Esta definición permite distinguir el ciberdelito "*stricto sensu*" de aquellos delitos clásicos que encuentran en la red su medio comisivo (*ad exemplum,* las amenazas, las vejaciones, injurias a través de correo electrónico, venta de droga, extorsión o amenazas vehiculizadas a través de internet, los delitos contra la libertad sexual etc).

TERCERA.- Cuando el ciberdelito se comete o produce sus efectos dentro del territorio del Estado Español, se reconoce la competencia para su persecución a favor del Juez de todos y cada uno de los lugares donde se manifiesten sus efectos, lo que incluye tanto el lugar de la acción como el del resultado. Este criterio sobre competencia territorial, conocido como principio de ubicuidad, se adoptó a partir del Acuerdo no jurisdiccional del Pleno del Tribunal Supremo de 3 de febrero de 2005, según el cual: "*el delito se comete en todas las jurisdicciones en las que se haya realizado algún elemento del tipo. En consecuencia, el Juez de cualquiera de ellas que primero haya iniciado las actuaciones procesales, será en principio competente para la instrucción de la causa"*.

CUARTA.- Como complemento al criterio inicial que establece el principio de ubicuidad, si conforme vaya avanzando la investigación de la causa llegara a determinarse el lugar geográfico concreto desde el que se introdujeron los datos delictivos en la red (ej. pornografía infantil), o el lugar en el que se produjo el daño, se destruyó el sistema operativo o se contaminaron los archivos (ej. injurias a través de internet o daños informáticos), cabe la inhibición a favor del Juez concreto conforme a la regla general del *forum delicti comisi* del art. 14 de la LECrim.

QUINTA.- Cuando se trate de ciberdelitos cometidos parcialmente en España los tribunales españoles del orden penal ostenta competencia para investigar y enjuiciar los aspectos de la acción ilícita que sea constitutiva de delito en España. Si surge un conflicto de jurisdicción entre Estados será de aplicación la Ley 16/2015, de 7 de julio, que recoge, por primera vez en nuestro derecho, parámetros específicos para la determinación de los criterios a tener en consideración a la hora de establecer la jurisdicción más adecuada en interés de la Justicia.

SEXTA.- A pesar de la producción de sus efectos lesivos, tratándose de ciberdelitos cometidos fuera del territorio nacional, la competencia de los Tribunales españoles se encuentra definida en el artículo 23 de la LOPJ. Como regla general los ciberdelitos no se consideran delitos de persecución universal en los términos del art. 23.4 de la citada Ley. No obstante, algunas modalidades delictivas sí que tendrían encaje en esa modalidad si van asociadas a fenómenos de tipo terrorista o siempre que así lo establezcan los correspondientes Tratados Internacionales, o cuando se trate de pornografía infantil (art. 189 del CP) de persecución universal en base a una doble vía: a) por ser uno de los delitos "relativos a la prostitución y/o corrupción de menores (art. 23.4-d LOPJ); o, b) por establecer el art. 189.1-b del CP para los de tráfico de material pornográfico infantil que es indiferente que el mismo tenga su origen en el extranjero o fuere desconocido.

SÉPTIMA.- El carácter transnacional del ciberdelito hace que en muchos casos sea necesario constituir equipos conjuntos de investigación o acudir a instancias internacionales para tratar de investigar los rastros dejados en el entorno informático, telemático o virtual o para solicitar diligencias necesarias para el aseguramiento de las pruebas. En el ámbito europeo habrá que acudir a la Orden Europea de Investigación, que establece un régimen único para la práctica de diligencias de investigación en otros Estados europeos, basada en el principio de reconocimiento mutuo y el derecho del Estado de ejecución, que a partir del 22 de mayo de 2017 sustituirá a otros convenios sobre la materia (Convenio Europeo de Asistencia Judicial en Materia Penal, hecho en Estrasburgo el 20 de abril de 1959, Convenio de aplicación del Acuerdo de Schengen de 19 junio de 1990 y Convenio Europeo relativo a la Asistencia Judicial en Materia Penal entre los Estados miembros de la Unión, hecho en Bruselas el 29 de mayo de 2000). Fuera del ámbito europeo habrá que acudir al régimen convencional existentes o, en su defecto, a la reciprocidad (277 LOPJ).

OCTAVA.- La colaboración de los ISP es esencial en la investigación de los ciberdelitos, al ser estos quienes disponen de los datos resultantes de cualquier interacción en el ciberespacio. Por ello vienen obligados tanto a un deber de conservación como al de prestar la colaboración exigida por la autoridad judicial, proporcionando dichos datos cuando les sean judicialmente requeridos, además de denunciar los contenidos delictivos que detecten en sus servidores y acordar el bloqueo de acceso o retiradas de contenidos o sitios web que se soliciten judicialmente (Ley 34/2002 de Servicios de la Sociedad de la Información y del Comercio Electrónico).

NOVENA.- Debido al uso de las nuevas tecnologías, la investigación de los ciberdelitos plantea la colisión o grado de injerencia en el ámbito de los derechos fundamentales del investigado. Los derechos de mayor afectación en los ciberdelitos son el derecho a la intimidad (18.1 CE), el derecho al secreto de las comunicaciones (18.3 CE), el derecho a la protección de datos de carácter personal (18.4 CE) y el denominado *derecho a la identidad virtual* cuyo germen doctrinal se encuentra en la STC 173/2011, de 7 de noviembre, que abarca una serie de elementos comunes a los

anteriores derechos fundamentales pero que precisamente por su interrelación alrededor de un mismo titular precisa de un tratamiento unitario.

DÉCIMA.- En la investigación del ciberdelito, los presupuestos aplicables para llevar a cabo una injerencia en los derechos fundamentales del artículo 18 de la CE, son los tradicionalmente establecidos según una doctrina consolidada jurisprudencial. A saber, se exige: *a)* la existencia de un fin constitucionalmente legítimo; *b)* la previsión legal de la medida limitativa del derecho; *c)* proporcionalidad de la medida definida a través del juicio de idoneidad, necesidad y proporcionalidad en sentido estricto; y *d)* la autorización judicial motivada salvo en los supuestos de consentimiento del afectado o de intervención policial por razones de urgencia y necesidad y siempre que, en este último caso, no exista reserva constitucional a favor de la autoridad judicial.

UNDÉCIMA.- Teniendo en cuenta el empleo de dispositivos tecnológicos, el consentimiento del afectado puede legitimar la injerencia en el derecho a la intimidad porque corresponde a cada persona acotar el ámbito de intimidad personal y familiar que reserva al conocimiento ajeno, aunque este consentimiento puede ser revocado en cualquier momento. Por ello se vulnera este derecho cuando la penetración en el ámbito propio y reservado del sujeto no sea acorde con la Ley, no sea eficazmente consentida, o cuando aún siendo expresamente autorizada, subvierta los términos y el alcance para el que se otorgó el consentimiento, quebrando la conexión entre la información personal que se recaba y el objetivo tolerado para el que fue recogida.

DUODÉCIMA.- La necesaria respuesta legal a muchos de los problemas prácticos que se planteaban por su complejidad en la investigación de los ciberdelitos se produjo con la reforma de la Ley de Enjuiciamiento Criminal operada por la Ley Orgánica 13/2015, de 5 de octubre. Dicha reforma legislativa vino a dotar de un marco legal preciso la práctica de diligencias de investigación relacionadas con las nuevas tecnologías.

DECIMOTERCERA.- Especialmente destacable resulta que la LECrim contemple una serie de técnicas de investigación tecnológicas que no precisan autorización judicial, pero que puede llevarlas a cabo la policía bajo el principio básico de que "*no se precisa autorización judicial para conseguir lo que es público",* con la finalidad de facilitar la investigación. A título de ejemplo, dichas medidas son: obtención de una IP, la identificación de los números MAC, IMEI e IMSI, la identificación de titulares o terminales o dispositivos de conectividad.

DECIMOCUARTA.- Sin contar *ex ante* con autorización judicial, determinadas diligencias resultarán justificadas cuando existan razones fundadas de urgencia y necesidad en las que se aprecie un interés constitucional legítimo y sea convalidada dicha actuación por autorización judicial *ex post.* En esta línea la LECrim permite que la policía pueda adoptar el registro de dispositivos, incluido el registro en la nube; a su vez, *e*l Ministro del Interior o, en su defecto, el Secretario de Estado de Seguridad*,* podrá ordenar la interceptación de las comunicaciones telefónicas y telemáticas cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas, en caso de urgencia y razones fundadas que hagan imprescindible esta medida. Ahora bien, la constatación *ex post* de la falta del presupuesto habilitante de estas dos últimas medidas implicaría la vulneración del derecho fundamental, por lo que tendría efectos procesales en cuanto a la ilicitud de la prueba en su caso obtenida.

DECIMOQUINTA.- La de intervención de las comunicaciones telemáticas, se presenta como una de las diligencias de investigación más invasivas desde el punto de vista de la afectación de los derechos fundamentales del investigado, a la par que una de las diligencias más complejas en cuanto a su ejecución y aportación del material intervenido al acto del juicio oral, ya que supone la interceptación y recopilación instantáneas de tanto de datos tráfico como de contenido.

DECIMOSEXTA.- La diligencia de intervención de las comunicaciones telemáticas suele enfrentarse a dos importantes problemas de orden práctico: *1)* en primer término, al tener la gran mayoría de las ISP (Hotmail, Yahoo, Gmail...) su sede en el extranjero -principalmente en EE.UU.-, la solicitud judicial de los datos que poseen debe acompañarse de una comisión rogatoria internacional, circunstancia que ralentiza la investigación. *2)* Desde que se ha activado en muchas de las aplicaciones los denominados cifrados de extremo a extremo o "protocolo severo" en los que sólo el emisor y el receptor pueden leer los mensajes o acceder a las llamadas, las compañías operadoras no tienen ninguna capacidad para intervenir los mensajes o llamadas de sus clientes, al no conocer la clave de cifrado, que es creada por el propio dispositivo. Por ello, el uso de estas nuevas técnicas de encriptación, obliga acudir a otras sofisticadas medidas de investigación tecnológica.

DECIMOSÉPTIMA.- Tanto por la importancia de la información albergada como por su privacidad, el ordenador (PC) y demás dispositivos informáticos (tabletas, teléfonos móviles) dejan de ser considerados como simples piezas de convicción, por lo que su registro exigirá un acto jurisdiccional habilitante, salvo en caso de urgencia. En este último supuesto, las injerencias policiales directas deberán ser examinadas con especial atención, pues algunas, como el acceso a los registros de llamadas o de mensajería no leída, exigen la previa autorización judicial en cuanto afectan al núcleo del derecho fundamental al secreto de las comunicaciones. Será necesario esperar a la autorización judicial, o si se trata de registros en la nube, solicitar la orden de conservación de datos regulada en el art. 588 octies LECrim, medida menos gravosa y garante de los derechos de las posibles personas afectadas.

DECIMOCTAVA.- La diligencia de registro remoto en la investigación del ciberdelito resulta especialmente destacable por su operatividad. Adviértase de que no se trata de un registro puntual, sino continuado en el tiempo, en el que mediante la utilización de claves o la instalación de troyanos, se realiza un control a distancia del equipo informático sin conocimiento de su titular. La singular injerencia de esta diligencia en los derechos fundamentales de los investigados obliga a extremar las

cautelas, motivo por el que su práctica requiere necesariamente la autorización judicial previa, se acotan con carácter de *numerus clausus* los delitos que la pueden habilitar, y se limita su duración temporal.

DECIMONOVENA.- Frente a determinados tipos delictivos (pornografía infantil, ciberterrorismo...), el agente encubierto virtual o informático actúa como un "espía" lícito en la red, mediante su infiltración en canales cerrados de comunicación con la pertinente autorización judicial, por lo que incluso puede intercambiar archivos ilícitos. Su actuación no se debe confundir con el marco de actuación policial en la red que puede realizarse sin necesidad de una previa autorización judicial, como es el caso del ciberpatrullaje o rastreos policiales realizados en fuentes abiertas, o la ocultación de la condición de policía, actuando como un usuario más de la red.

VIGÉSIMA.- Resulta acertada la regulación positiva de los denominados hallazgos casuales que pudieran surgir con motivo de la adopción y práctica de distintas medidas de investigación tecnológica. Aunque la jurisprudencia había admitido la validez de los hallazgos casuales, la continuidad de la investigación ante un hecho delictivo nuevo requerirá de una renovada autorización judicial que legitime la diligencia en cuya práctica se produce dicho hallazgo casual, lo que no será infrecuente en el ámbito de investigación de los ciberdelitos.

VIGESIMOPRIMERA.- Las peculiaridades en torno a la prueba de los ciberdelitos vienen suscitadas por la propia singularidad de su comisión, al tener lugar en un ámbito inmaterial como es el espacio virtual, constituido por las redes telemáticas. En el espacio virtual la información y acreditación del hecho no sólo viene representado por datos electromagnéticos, eminentemente volátiles, sino que tanto su comisión como su constatación por el ser humano precisa de unos elementos físicos, constituidos por los propios equipos informáticos y telemáticos. Estas circunstancias acrecientan tanto las dificultades para la obtención del material probatorio como el aseguramiento del mismo.

VIGESIMOSEGUNDA.- Por prueba informática se entiende la información generada, almacenada o transmitida mediante el uso de dispositivos informáticos que tiene aptitud para acreditar el hecho objeto de enjuiciamiento y formar la convicción judicial. La fuente de la prueba radica en la información contenida o transmitida por medios informáticos, mientras que el medio de prueba se refiere al modo a través de la cual esa información entra en el proceso: normalmente como prueba documental o como prueba pericial, pero también incluso a través de la prueba testifical mediante el testimonio de la persona que ha tenido contacto con el dispositivo informático.

VIGESIMOTERCERA.- La prueba informática está sometida a un doble juicio respecto a sus requisitos de admisibilidad: *a)* un previo **juicio de licitud** para garantizar que la prueba se haya obtenido sin violar derechos fundamentales, pues de lo contrario, sería nula; y *b)* un **juicio de fiabilidad**, que garantice la autenticidad (no manipulación) y la integridad (conservación del contenido) del material aportado, la intangibilidad e inalterabilidad del mismo y la ausencia de técnicas espurias en la obtención de la información recabada a través de los concretos medios de investigación empleados.

VIGESIMOCUARTA.- Para garantizar la fiabilidad de las pruebas informáticas la LECrim establece unas prescripciones que han de seguirse en la adopción de las medidas de investigación tecnológica. Se habrán de poner en conocimiento del órgano jurisdiccional la utilización de los artificios empleados para la captación de códigos, las concretas medidas adoptadas para asegurar la autenticidad e integridad de los datos, el sellado tecnológico del archivo en la interceptación de las comunicaciones, el clonado o volcado de datos, y el control sobre las medidas, en especial sobre el archivo ilícito que el agente encubierto pretende enviar para su posterior recuperación y para evitar el riesgo de que incurra en provocación delictiva.

VIGESIMOQUINTA.- Al igual que el conjunto del material probatorio, la prueba informática deberá valorarse según el principio de "intima convicción o apreciación en conciencia" del art. 741 LECrim. Pero con frecuencia la complejidad de esta prueba hará necesario contar con un dictamen pericial informático para autentificar contenidos en redes sociales (como Facebook, Twitter, Tuenti), o incluso cuando se trate de mensajes intercambiados a través de WhatsApp y demás mensajería, si se impugna su autenticidad. Pese a su enorme importancia en los ciberdelitos, la valoración judicial de la pericia deberá realizarse en función de las circunstancias del caso, al estar motivada la intervención del perito en la ausencia de conocimientos técnicos especializados por parte del tribunal.

APÉNDICE NORMATIVO

En este anexo se trata la normativa dictada en el ámbito internacional, europeo y nacional relacionada con el ciberdelito y con sus aspectos procesales, pues una visión general de la misma facilita el estudio de su investigación y prueba.

Hay que tener en cuenta el Código del Derecho a la Ciberseguridad[684] donde se se recogen normas que afecten directamente a esta materia para facilitar su necesario estudio y análisis. Dentro de este compendio de normas merece una mención especial por su afección a la investigación y prueba, las siguientes:

1. NORMATIVA DE ÁMBITO INTERNACIONAL.

Hay que destacar en el ámbito universal la ONU[685] y la OCDE han estado activas en este ámbito discutiendo en foros internacionales sobre el tratamiento procesal de los ciberdelitos y elaborando directrices para la seguridad de los sistemas de información. Aunque sin duda el Instrumento más importante internacionalmente es el Convenio sobre Ciberdelincuencia, que tomó como referencia las conceptuaciones, posicionamientos, y conclusiones contenidas en los textos normativos precedentes y antecedentes doctrinales en el marco de la Unión Europea y del Consejo de Europa[686].

[684] Publicado en BOE nº 173, de fecha 12 de agosto de 2016. Autor: Pérez Bes, Francisco. Secretario General del Instituto Nacional de Ciberseguridad de España, S.A. (INCIBE)

[685] http://www.un.org/es/events/crimecongress2015/about.shtml. Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente que se celebra cada cinco años y reúne a los encargados de la formulación de políticas y los profesionales que se ocupan de la prevención del delito y la justicia penal para elaborar las normas de las Naciones Unidas sobre prevención del delito y justicia penal una de los cursos prácticos es el dedicado a los Delitos relacionados con las redes informáticas.

[686] Preámbulo del Convenio sobre ciberdelincuencia. https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_spanish.PDF.

1. 1. Convenio sobre Ciberdelicuencia.

El Convenio sobre la Ciberdelincuencia del Consejo de Europa[687] hecho en Budapest el 23 de noviembre de 2001[688], ratificado por España el 20 de mayo de 2010, implica por su carácter imperativo un punto de inflexión hacia un tratamiento penal sustantivo, autónomo, unificado y extensivo del fenómeno de la ciberdelincuencia[689].

Dicho Tratado se constituye realmente en el primer instrumento multilateral dirigido a sentar las bases para afrontar los problemas planteados por la expansión de la actividad criminal en las redes informáticas, puesto que en la mayoría de los países se habían dedicado escasa, cuando no nula, atención a las dificultades inherentes a la aplicación al mundo virtual de las normas sobre investigación diseñadas para el mundo físico[690]. Por ello, se requiere a los Estados firmantes la promulgación de leyes contra la ciberdelincuencia, materializándola en normas y tipos penales para asegurar que los agentes y autoridades públicas tengan la capacidad procesal necesaria para investigar y perseguir con efectividad este tipo de delitos, y normas que promuevan la cooperación internacional con otros estados en la lucha contra el ciberdelito[691].

Es un instrumento jurídico a través del que se pretende establecer, con vocación de universalidad, las bases de una política penal común contra este fenómeno criminal. Los pilares sobre los que se asienta este acuerdo son precisamente la armonización

[687] El texto completo del Convenio en inglés o francés es accesible a través de la página web del Consejo de Europa http.//conventions.coe.int/treaty. La traducción en español la he obtenido en el siguiente enlace Council of Europe (ETS no. 185), Convenio sobre cibercriminalidad http://conventions.coe.int/Treaty/en/Treaties/html/185-SPA.htm.

[688] Entró en vigor el 1 de julio de 2004 tras ser ratificado por 22 Estados (España lo hizo por Instrumento de 20 de mayo de 2010 (BOE de 17 de septiembre de 2010, y entró en vigor en España el 1 de octubre de 2010).

[689] ROVIRA DEL CANTO, E. Nuevas formas de ciberdelincuencia intrusiva: el hacking y el grooming. Iuris: Actualidad y práctica del derecho nº 160, 2011 págs. 36-44.

[690] LEZERTUA RODRÍGUEZ, M. El proyecto de Convenio sobre el Cibercrimen del Consejo de Europa, ob. cit. pág. 44.

[691] 51 Estados han ratificado el Convenio a fecha 8 de enero de 2017. http://www.coe.int/en/web/conventions/full-list//conventions/treaty/185/signatures?p_auth=VQYg4M0R. 8/1/2017 a las 12.00

penal sustantiva y procesal y el reforzamiento de los mecanismos de cooperación internacional[692].

Desde el punto de vista del Derecho Penal material establece una novedosa clasificación por grupos de los ciberdelitos, que se complementan con los previstos en el Protocolo adicional relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos[693].

Los aspectos procesales del Convenio (sección segunda de su capitulo II) tienen como objetivo establecer criterios comunes que hayan de ser asumidos por todos los Estados firmantes. Se establece una serie de mínimos y bases normativas referentes a la obtención, conservación y presentación de pruebas informáticas fiables ante los tribunales de justicia.

Los medios de investigación que prevé expresamente, son:

a) La conservación inmediata de los datos informáticos almacenados (artículo 16).
b) La conservación inmediata y revelación parcial de datos de tráfico (artículo 17).
c) El mandato de exhibición (artículo 18).
d) El registro y decomiso de datos informáticos almacenados (artículo 19).
e) y por último, la obtención e interceptación en tiempo real de datos de tráfico (artículo 20) y de datos de contenido (artículo 21).

Por otro lado, es de señalar que el Texto se refiere en general a todo tipo de datos, pero especificando tres tipos de datos informáticos: datos de tráfico, datos de contenido y datos de abonado; así como que los mismos pueden existir en dos formas: almacenados o en el proceso de comunicación; y en consecuencia, la aplicabilidad de

[692] ROVIRA DEL CANTO, E. "Las nuevas pruebas telemática y digitales (…) ob. cit. págs. 277-326.

[693] Protocolo Adicional al Convenio (ETS N.O 189) relativo a la Criminalización de los Actos de Naturaleza Racista y Xenófoba cometidos a través de Sistemas Informáticos, hecho en Estrasburgo el 28 de enero de 2003, que entró en vigor el 1 de marzo de 2006. El 11 de noviembre de 2014, España ratificó este Protocolo Adicional, habiéndose publicado el instrumento de ratificación en el BOE de día 30 de enero de 2015.

las medidas o procedimientos que recoge el Convenio a uno u otro tipo o forma de datos electrónicos en particular, dependerá de la naturaleza y forma no sólo del dato sino también de la propia naturaleza del procedimiento descrito en cada artículo.

Por último, el capítulo III del CSC -dedicado a la Cooperación Internacional- , establece un conjunto de principios para la elaboración de un régimen jurídico internacional en las investigaciones sobre los ciberdelitos. Se examina la importancia creciente de la cooperación internacional (artículos 23 a 35 CSC) y se promueve el uso de medios de comunicación expeditos, como el fax y el correo electrónico (artículo 25, párrafo 3). Además, se insta a las partes en el Convenio a que designen un punto de contacto disponible las 24 horas del día, todos los días de la semana, para responder a las solicitudes de asistencia de los Estados (artículo 35 CSC). Se stablece un procedimiento para el caso de que no haya entre los Estados (art. 27 CSC). De gran importancia para la investigación de los ciberdelitos son las medidas establecidas en la Sección 2 del Capítulo III del Convenio de ciberdelincuencia sobre la asistencia en materia de medidas cautelares, tales como la conservación inmediata de datos informáticos almacenados (art. 29 CSC), la comunicación inmediata de los datos informáticos conservados (art. 30 CSC), sobre la asistencia en relación a los poderes de investigación concerniente al acceso a datos informáticos almacenados (art. 31 CSC), al acceso transfronterizo a los datos informáticos almacenados, con consentimiento o de libre acceso (art. 32 CSC), a la asistencia para la recogida en tiempo real de datos de tráfico (art. 33 CSC) y por último a la asistencia en materia de interceptación de datos relativos al contenido (art. 34 CSC).

2. NORMATIVA DE ÁMBITO EUROPEO[694].

En el ámbito europeo, la ciberdelincuencia figura entre los diez delitos graves con dimensión transfronteriza recogidos en el artículo 83.1 del TFUE[695], y de ahí que cada vez sea mayor el número de iniciativas y actuaciones destinadas a prevenir y combatir la ciberdelincuencia en la Unión Europea.

Estas actuaciones tienen como principal objetivo armonizar el derecho penal sustantivo en el ámbito de la ciberdelincuencia[696].

No existen instrumentos jurídicos de la UE que aborden directamente la delincuencia informática, pero sí existen diversos instrumentos jurídicos que tratan indirectamente la cuestión. Son varias las normas dictadas para la creación de lo que podríamos llamar un Derecho penal europeo en materia de ciberdelincuencia. Lo que sí llama la atención es que todo el movimiento armonizador ha tenido más como objetivo el derecho penal sustantivo de la Unión Europea que el derecho procesal, con la excepción de la Directiva 2014/41/UE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal[697], que aún no ha sido traspuesta a nuestro derecho interno.

De entre las acciones legislativas tomadas en el ámbito de la UE para luchar contra la ciberdelincuencia, cabe señalar[698]:

---

[694] El listado exacto de la normativa aprobada en la Unión Europea lo podemos encontrar en la siguiente página: http://www.informatica-juridica.com/legislacion/union-europea/

[695] Artículo 83 TFUE (antiguo artículo 31 TUE). www.eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:12012E/TXT

[696] RCL 2009, 2289. El movimiento de armonización del Derecho penal en la Unión Europea tomó un giro más decidido a partir de la firma del Tratado de Lisboa de 13 de diciembre de 2007, al optarse por la Directiva en vez de por la Decisión Marco, a fin de conseguir mayor eficacia para avanzar en la armonización de disposiciones relativas a las infracciones con dimensión transfronteriza de especial gravedad, entre las que se encuentra la ciberdelincuencia.

[697] DO L 130 de 1.5.2014, p. 1. Aunque esta Directiva más que armonizar el derecho procesal de los países miembros, se centra en el principio de confianza legítima, y en la necesidad de dar validez a las diligencias practicadas en otro país siempre que sean conformes a su derecho. El derecho que se aplica, por tanto, es derecho del Estado de ejecución.

[698] Resulta de interés conocer las directivas vigentes, debido al lugar preeminente que el derecho comunitario ocupa dentro del sistema de fuentes, de manera que si el derecho nacional vulnera el comunitario, el ordenamiento comunitario contempla mecanismos de control: Recurso de incumplimiento

2.1 Directiva 2000/31/Ce del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados Aspectos Jurídicos de los Servicios de La Sociedad de La Información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).

Esta directiva es importante porque modifica la responsabilidad de los proveedores de servicios intermediarios sobre determinadas actividades y prohíbe a los Estados miembros imponerles una obligación general de supervisar los datos que transmitan o almacenen. Fue traspuesta por Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

2.2 Decisión Marco del Consejo, de 28 de Mayo de 2001, Sobre La Lucha Contra el Fraude y la Falsificación de Medios de Pago Distintos del Efectivo[699].

El enfoque de la presente Decisión marco fue evitar el recurso a calificaciones estrictamente definidas en el Derecho Penal y se limitó a elaborar una lista de los distintos comportamientos que deben considerarse como infracciones penales en toda la Unión[700].

2.3 Directiva 2002/58/Ce Del Parlamento Europeo y del Consejo de 12 de Julio de 2002, relativa al Tratamiento de Datos Personales y a la Protección de la Intimidad en el Sector de las Comunicaciones Electrónicas. (Directiva Sobre la Privacidad y las Comunicaciones Electrónicas)[701].

Dicha directiva estableció normas para garantizar la seguridad en el tratamiento de los datos personales, la notificación de sus violaciones y la confidencialidad de las

---

(arts. 226-228 TCE); Recurso de anulación (arts. 230, 231 y 233 TCE); Cuestión prejudicial (art. 234 TCE).

[699] Framework Decision on combating fraud and counterfeiting . http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV:l24212

[700] MORALES GARCÍA, O. *Delincuencia informática: intrusismo, sabotaje informático y uso ilícito de tarjetas (arts.197.3 y 8, 264 y 248)*, en "La Reforma Penal de 2010: Análisis y Comentarios" dirigidos por Gonzalo Quintero Olivares, Ed. Thomson Aranzadi Reuters, 2010.

[701] ePrivacy Directive http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:l24120

comunicaciones. Asimismo, prohibió las comunicaciones en las que el usuario no ha dado su consentimiento.

Los países de la UE deben garantizar la confidencialidad de las comunicaciones realizadas a través de las redes públicas y deben determinar el régimen de sanciones, incluidas las penales, en caso de violación. Dicha directiva fue traspuesta en Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones (derogada por Ley 9/2014, de 9 de mayo, General de Telecomunicaciones).

2.4 Directiva 2006/24/Ce del Parlamento Europeo y del Consejo Sobre la Conservación de Datos Generados o Tratados en Relación con la Prestación de Servicios De Comunicaciones Electrónicas de Acceso Público o de Redes Públicas de Comunicaciones.

El objeto de esta Directiva era establecer la obligación de los operadores de telecomunicaciones de retener determinados datos generados o tratados por los mismos, con el fin de posibilitar que dispongan de ellos los agentes facultados en casos detección o investigación por delitos graves, definidos éstos de acuerdo con la legislación interna de cada Estado miembro. Al respecto, los Estados Miembros adoptarían las medidas oportunas para que únicamente se proporcionaran los datos conservados a las autoridades competentes en supuestos específicos y de acuerdo con la normativa nacional. Esta Directiva fue declarada inválida el 8 abril 2014, por el Tribunal de Justicia de la Unión Europea[702].

Fue objeto de trasposición a la legislación española por Ley 25/2007, de 18 de Octubre, de Conservación de Datos Relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones, vigente pese a la invalidación de la directiva de la que traía su objeto.

[702] Sentencia en los asuntos acumulados C-293/12 y C-594/12 Digital Rights Ireland y Seitinger y otros - EDJ 2014/68463.

2.5 Directiva 2011/93/UE, Relativa a la Lucha contra los Abusos Sexuales y la Explotación Sexual de los Menores y la Pornografía Infantil[703].

Sustituyó a la Decisión Marco 2004/68/JAI relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil, unificó en toda la Unión Europea las infracciones penales relativas a los abusos sexuales sobre menores, su explotación sexual y la pornografía infantil y estableció disposiciones conducentes a luchar contra la pornografía infantil a través de internet[704].

La incorporación de la Directiva 2011/93 se efectuó en la Ley Orgánica 1/2015, de 30 de marzo, por la que se modificó el Código Penal[705].

2.6 Directiva 2012/29/Ue del Parlamento y del Consejo, de 25 De Octubre De 2012, por la que se Establecen Normas Mínimas Sobre Los Derechos, El apoyo y la Protección De Las Víctimas De Delitos.

Sustituye la Decisión marco 2001/220/JAI del Consejo, Se ocupa muy particularmente del derecho a la intimidad de las víctimas y de sus familias, así como de la utilización de las TIC en los procesos penales lo que resultará de gran utilidad también para las víctimas (fundamentalmente menores de edad) de la ciberdelincuencia[706]. La trasposición se ha llevado a cabo en la ley 4/2015, de 27 de abril, del Estatuto de la Víctima del Delito, que modifica la Ley de Enjuiciamiento Criminal.

[703] DO L 335 de 17.12.2011, p. 1. (fin de plazo de incorporación al Derecho nacional: 18 de diciembre de 2013) A Directive on combating the sexual exploitation of children online and child pornography

[704] http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV:jl0064

[705] *vid.* el apartado XII de la Exposición de Motivos de la citada Ley Orgánica explica de forma detallada la regulación que se incorpora al Ordenamiento español.

[706] http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:jl0027.

2.7 Directiva 2013/40, relativa a los Ataques contra los Sistemas de Información[707] .

Sustituyó a la Decisión marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, introdujo nuevas normas para armonizar la criminalización y las penas de los delitos contra los sistemas de información que abarcó desde ataques de denegación de servicio, concebidos para dejar fuera de servicio un servidor, hasta la interceptación de datos y ataques de botnets.

La incorporación de la Directiva se efectuó en la Ley Orgánica 1/2015, de 30 de marzo, por la que se modificó el Código Penal[708].

2.8 Directiva 2014/41/UE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal[709].

De gran importancia para la investigación del ciberdelito es la orden europea de investigación (OEI) pues establece un régimen único para la obtención de pruebas en los casos de dimensión transfronteriza[710].

[707] DO L 218 de 14.8.2013, p. 8)fin de plazo de incorporación al Derecho nacional: 4 de septiembre de 2015) A Directive on attacks against information systems Sustituye a Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información.

[708] El apartado XIII de la Exposición de Motivos de la citada Ley Orgánica explica de forma detallada la regulación que se incorpora al Ordenamiento español.

[709] DO L 130 de 1.5.2014, p. 1

[710] La Exposición de Motivos de la Directiva 2014/41/UE señala que mediante el Programa de Estocolmo, de diciembre de 2009, el Consejo decidió proseguir con la creación de un sistema general para obtener pruebas en los casos de dimensión transfronteriza, basado en el principio de reconocimiento mutuo. Ciertamente, los instrumentos existentes en este ámbito constituían un régimen fragmentario y que había que ir hacia un nuevo planteamiento basado en el principio de reconocimiento mutuo y que tuviera en cuenta la flexibilidad del sistema de asistencia judicial. Así, el Consejo abogó por un sistema general que sustituyera a todos los instrumentos existentes en este ámbito y que cubra, en la medida de lo posible, todos los tipos de pruebas, contenga plazos para su aplicación y limite en la medida de lo posible los argumentos para la denegación. Este nuevo planteamiento se basa en un único instrumento denominado orden europea de investigación que se expedirá a efectos de obtener una o varias medidas de investigación específicas que se llevarán a cabo en el Estado de ejecución de la OEI con vistas a la obtención de pruebas. Esto incluye la obtención de pruebas que ya están en posesión de la autoridad de ejecución (*vid*. arts. 6 y 7). Mediante dicha directiva se establecen normas para la práctica de una medida de investigación en cualquiera de las fases del procedimiento penal, incluida la vista, si es preciso con la participación del interesado, a efectos de la obtención de pruebas.

La OEI viene definida como aquella "resolución judicial emitida o validada por una autoridad judicial de un Estado miembro (el Estado de emisión) para llevar a cabo una o varias medidas de investigación en otro Estado miembro (el Estado de ejecución) con vistas a obtener pruebas con arreglo a la presente Directiva. También se podrá emitir una OEI para obtener pruebas que ya obren en poder de las autoridades competentes del Estado de ejecución"[711].

La OEI se ejecutará en cada Estado miembro sobre la base del principio de reconocimiento mutuo y se regirá por el derecho del estado de ejecución[712].Existiendo un mínimo de diligencias que se podrán pedir a cualquier estado miembro (información o de pruebas que obren ya en poder de la autoridad de ejecución; información contenida en bases de datos directamente accesibles a la autoridad de ejecución; declaración de un testigo, un perito, una víctima, un investigado o acusado o un tercero en el territorio del Estado de ejecución; cualquier medida de investigación no invasiva definida con arreglo al Derecho nacional del Estado de ejecución; identificación de personas que sean titulares de un número de teléfono o una dirección IP determinados)[713].

La OEI se puede transmitir por cualquier medio que deje constancia escrita de su autenticidad y de las fechas de envío y recepción[714]. Debe ser necesaria, proporcionada[715], respetuosa de los derechos del sospechoso o acusado y ajustada a las condiciones de una medida semejante en el orden interno (art. 6). Para controlar su utilización el art. 14 establece un sistema de recursos. La medida de investigación se

[711] Los equipos conjuntos de investigación están expresamente excluidos del ámbito de la Directiva, y continuarán rigiéndose por las normas actualmente vigentes.

[712] El art. 9.1 establece que la autoridad de ejecución deberá reconocer una OEI sin requerir otra formalidad y se asegurará de que se ejecute de la misma manera y bajo las mismas circunstancias que si la medida de investigación de que se trate hubiera sido ordenada por una autoridad del Estado de ejecución, salvo que la autoridad de ejecución decida invocar alguno de los motivos de denegación del reconocimiento o de la ejecución de la OEI (-vid. art. 11), o alguno de los motivos de aplazamiento contemplados en la Directiva.

[713] Artículo 10 de la Directiva, estas Diligencias tienen que existir en el Derecho nacional del Estado de ejecución, no cabe denegar su práctica.

[714] Un formulario anexo a la Directiva permite documentar la OEI sin dificultad. En principio, la transmisión es directa entre autoridades judiciales, aunque algunos países podrán designar autoridades centrales (en todo caso para asistir a los órganos judiciales y, excepcionalmente, para ocuparse directamente de la transmisión y recepción).

[715] Por ejemplo no cabe solicitar una detención para practicar una declaración.

llevará a cabo con la misma celeridad y prioridad que en casos internos similares y, en cualquier caso, dentro de los límites temporales previstos en el art. 12 [716].

Los Estados miembros deben haber transpuesto lo dispuesto en esta Directiva para el 22 de mayo de 2017[717], fecha en la que según se establece en el art. 34, la Directiva sustituye a diversas disposiciones correspondientes de convenios aplicables a las relaciones entre los Estados miembros vinculados por la Directiva[718].

---

[716] En la Directiva hay disposiciones detalladas sobre determinadas medidas de investigación (traslados temporales, informaciones bancarias, video y teleconferencias, intervención de telecomunicaciones, etc.) en los arts. 22 a 31
El artículo 30 de la Directiva es el dedicado a la Intervención de telecomunicaciones con la asistencia técnica de otro Estado miembro
"1. Se podrá emitir una OEI para la intervención de telecomunicaciones en el Estado miembro cuya asistencia técnica se requiera.
2. Cuando haya más de un Estado miembro que esté en situación de proporcionar la asistencia técnica completa necesaria para la misma intervención de telecomunicaciones, la OEI se enviará a uno solo de ellos, y se dará prioridad siempre al Estado miembro en que se encuentre o vaya a encontrarse la persona que sea objeto de los procedimientos penales
3. Una OEI de las previstas en el apartado 1 incluirá también la siguiente información:
a) aquella que sea necesaria para identificar a la persona objeto de la intervención
b) duración deseada de la intervención y
c) datos técnicos suficientes, en particular el identificador de la persona, a fin de garantizar que pueda ejecutarse la solicitud.
4. En la OEI, la autoridad de emisión indicará las razones por las que estima que la medida de investigación indicada es pertinente para el procedimiento penal en cuestión.
5. Podrá denegarse la OEI, además de por los motivos que se refiere el artículo 11, si la ejecución de la medida de investigación no estuviera autorizada en casos internos similares. El Estado miembro de ejecución podrá supeditar su consentimiento a las condiciones que regirían en un caso interno de características similares.
6. Una OEI de las previstas en el apartado 1 podrá ejecutarse mediante:
a) la transmisión inmediata de las telecomunicaciones al Estado de emisión, o
b) la intervención, registro y ulterior transmisión del resultado de la intervención de las telecomunicaciones al Estado de emisión.
La autoridad de emisión y la autoridad de ejecución mantendrán consultas con el fin de acordar si la intervención habrá de efectuarse con arreglo a la letra a) o a la letra b).
7. A la hora de emitir una OEI con arreglo al apartado 1, o bien durante la intervención, la autoridad de emisión podrá pedir asimismo, si tiene motivos particulares para hacerlo, una transcripción, descodificación o desencriptado del registro, siempre que cuente con el acuerdo de la autoridad de ejecución.
8. Los gastos que resulten de la aplicación del presente artículo se sufragarán con arreglo al artículo 21, salvo los que se deriven de la transcripción, la descodificación y el desencriptado de las comunicaciones intervenidas, que correrán a cargo del Estado de emisión.

[717] Art. 36 de la Directiva.

[718] A partir del 22.5.217 la presente Directiva sustituye:
a) Convenio Europeo de Asistencia Judicial en Materia Penal del Consejo de Europa, de 20 de abril de 1959, así como sus dos protocolos adicionales y los acuerdos bilaterales celebrados con arreglo a su art. 26; b) Convenio relativo a la aplicación del acuerdo de Schengen; c) Convenio relativo a la asistencia judicial en materia penal entre los EM de la UE y su Protocolo(Decisión)
-Queda sustituida la Decisión Marco 2008/978/JAI para todos los Estados miembros vinculados por la presente Directiva.

2.9 Reglamento Europeo de Protección de Datos (Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016).

Este Reglamento por el que se deroga a la Directiva 95/46/CE (Reglamento General de Protección de datos), constituye la norma fundamental de la Unión Europea en materia de protección de datos personales y de la libre circulación de los datos aplicable al territorio de la UE y a sus ciudadanos. Es una norma de efecto directo que no requiere transposición al derecho interno, y que armoniza las legislaciones existentes hasta ahora en los Estados Miembros. Entró en vigor el 26 de mayo de 2016 y será de aplicación a partir del 25 de mayo de 2018[719]. Destacar que en el artículo 23 se establece que cualquier medida legislativa que limite este derecho fundamental (y entre ellas obviamente está la que establece la obligación de las operadoras de conservar los datos de tráfico) debe cumplir con los siguientes requisitos: debe expresar la finalidad del tratamiento de datos; determinar las categorías de datos personales objeto de tratamiento; el alcance de las limitaciones establecidas; las garantías para evitar accesos o transferencias ilícitas o abusivas de los datos tratados; la determinación de un responsable que vigile dicha actividad; los plazos de conservación y las garantías aplicables según la naturaleza y objetivos del tratamiento o las categorías de datos afectados; disposiciones relativas a los riesgos para los derechos y libertades de los interesados y el derecho de los interesados a ser informado sobre la limitación, excepto en el supuesto de que tal información pueda perjudicar la finalidad de la limitación.

2.10 Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016.

Relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (conocida como Directiva NIS, *Network and Information Security*). Deberá estar traspuesta al derecho interno de los Estados miembros el 9 de mayo de 2018.

-La Decisión Marco 2003/577/JAI queda sustituida para todos los Estados miembros vinculados por la presente Directiva en relación con el aseguramiento de pruebas. Para los Estados miembros vinculados por la presente Directiva, las referencias de la Decisión marco 2008/987/JAI y, en lo que respecta a la inmovilización de activos, a la Decisión marco 2003/577/JAI, se entenderán hechas a la presente Directiva.

[719] BACARIA MARTRUS, J. "Las novedades del Reglamento General Europeo de Protección de Datos". Revista Economist & Jurist nº 201. Ed. Difusión Jurídica y Temas de Actualidad. Madrid 2016. Págs 16 a 27.

3. LEGISLACIÓN NACIONAL.

3.1 La Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

El Código Penal no contempla (ni en su redacción original ni en las sucesivas modificaciones) un título específico dedicado a los ciberdelitos. Los distintos ciberdelitos, se encuentran desperdigados en su articulado (arts. 186, 197, 211, 238.5, 248.2 y 3, 256, 270, 286, etc.), sin más orden que su ubicación en distintos capítulos, en función de los bienes jurídicos en los que se ha decidido incluirlos. No se considera, pues, que exista ningún vínculo común entre ellos[720]. En consecuencia, en el CP español "tras su aprobación" recogía como ciberdelitos los siguientes: arts. 186-189 (Pornografía infantil); art. 197.2 (espionaje informático); art. 211 (Injurias y calumnias a través de la red); art. 238.5 (Robo inutilizando sistemas de guarda criptográfica); art. 248.2 (estafa informática); art. 256 (ubicación abusiva de equipos terminales de telecomunicación); art. 264.2 (sabotaje o daños informáticos); art. 270 (propiedad intelectual); arts. 273-275 (contra la propiedad industrial); art.278.1 (secretos de empresa); art.286 (uso ilegal de equipos, programas y servicios informáticos); art. 402 (usurpación de funciones públicas por correo); arts. 417-418 y 423 (infidelidad en la custodia de documentos y violación de secretos); art. 560.1 (ataques a líneas o instalaciones de telecomunicación o correspondencia postal) y arts. 598 y 603 (descubrimiento y revelación de secretos relativos a la Defensa Nacional)[721]

Dos reformas importantes sufrió el Código en materia de ciberdelitos: *una de ellas en año 2010 por la LO 5/2010, de 22 de Junio*[722], que motivada por la necesidad de cumplir con previas obligaciones internacionales contraídas por España[723] introdujo

[720] DE URBANO CASTRILLO, E. "Los delitos informáticos tras la reforma del CP de 2010". ob. cit. pág.1. "*Dicho panorama reclamaba una reforma y se esperaba con cierta esperanza que en la primera ocasión posible pudieran solucionarse estos problemas. La situación, como se verá, ha mejorado pero puede sostenerse, sin duda alguna, que la reforma ha defraudado las expectativas existentes"*.

[721]DE URBANO CASTRILLO, E. "Los delitos informáticos tras la reforma del CP de 2010". ob. cit. pág. 2.

[722] BOE 23 de junio de 2010. con entrada en vigor el 24-12-2010.

[723] La justificación de la reforma en materia de ciberdelitos, fue adaptar nuestra legislación al Convenio de Ciberdelincuencia que al ser ratificado por España entraba en vigor en el año 2010 y cumplimentar la

nuevos tipos y reformó algunos ya existentes. Así, los tres principales delitos informáticos afectados por esta reforma fueron, el "hacking" o intrusión informática (art.197 CP) que se reguló por primera vez[724], la estafa informática (art.248 CP)[725] y el "cracking" o daños informáticos, previsto en el art. 264 CP[726]. Con ellos, la reforma afectó también a otras modalidades delictivas relacionadas con internet, se añadió un nuevo artículo 183 bis, se modificó el artículo 189, se añadió un artículo 189 bis, subtipo especial para los delitos comprendidos en el capítulo V (Prostitución y Corrupción de Menores), cuando el responsable sea una persona jurídica. En el llamado robo tecnológico se modificó el artículo 239 para añadir al concepto de "llave falsa" el de "cualquier otro instrumento tecnológico de eficacia similar" y se retocaron los delitos contra la propiedad intelectual e industrial, que podían cometerse utilizando cualquier soporte, y por lo tanto, el electrónico, así como atentando a las cibermarcas.

La otra reforma importante en el Código Penal en materia de ciberdelitos tuvo lugar en el año 2015, a través de dos leyes:

- *por la Ley Orgánica 1/2015, de 30 de marzo*[727]*,* que llevó a cabo la transposición de la de la Directiva 2011/93/UE relativa a la lucha contra los abusos

---

Decisión Marco 2005/222/JAI, de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información.

[724] DE URBANO CASTRILLO, E "Los delitos informáticos tras la reforma del CP de 2010 ". ob. cit. pág. 3. "*La reforma introdujo el llamado "hacking blanco", consistente en el acceso inconsentido a informaciones ubicadas en el sistema informático (datos, programas...) o el simple mantenimiento en páginas web ajenas, sin consentimiento del titular, sin necesidad de móvil o acción posterior alguna, se sanciona con pena de hasta dos años.*
Se castiga, pues, el mero hecho de saltarse las barreras de seguridad informáticas, como un atentado al derecho a la "intimidad informática" pero siempre que exista un acceso a los datos o programas albergados.

[725] DE URBANO CASTRILLO, E. "Los delitos informáticos tras la reforma del CP de 2010". ob. cit. pág. 4. "*La reforma en este punto, supuso una ampliación de la estafa informática que ya estaba tipificada, y se añadieron a las conductas existentes hasta ahora, otras de naturaleza económica en la que el engaño se canaliza a través de la informática. En concreto, se castiga como "estafa informática", la utilización de tarjetas de crédito o débito o cheques de viaje para realizar operaciones de cualquier clase en perjuicio del titular de dichoso instrumentos de pago o de terceros".*

[726] DE URBANO CASTRILLO, E. "Los delitos informáticos tras la reforma del CP de 2010". ob. cit. pág. 4. "*En relación a los "daños informáticos" se amplían las conductas punibles, con la obstaculización de un sistema informático ajeno –entre otros medios- introduciendo datos informáticos sin autorización y se agrava la pena cuando el autor sea una organización criminal, la conducta sea de especial gravedad o quepa atribuir responsabilidad penal a una persona jurídica".*

[727] Publicada en el Boletín Oficial del Estado de 31 de marzo de 2015, con entrada en vigor el 1 de julio de 2015.

sexuales y la explotación sexual de los menores y la pornografía infantil, y la trasposición de la Directiva 2013/40/UE, de 12 de agosto, relativa a los ataques contra los sistemas de información y la interceptación de datos electrónicos cuando no se trata de una comunicación personal. Las modificaciones propuestas pretendían superar las limitaciones de la regulación para ofrecer respuesta a la ciberdelincuencia en el sentido de la normativa europea.

- *y por la Ley Orgánica 2/2015, de 30 de marzo*, [728] *en materia de delios de terrorismo*[729].

3.2 Ley de Enjuiciamiento Criminal.

La nuevas formas de delincuencia ligadas al uso de las nuevas tecnologías pusieron de manifiesto la insuficiencia de la Ley de Enjuiciamiento Criminal de 1882, que no ha podido sustraerse al paso del tiempo.

Los flujos de información generados por los sistemas de comunicación telemática advertían de las posibilidades que se hallaban al alcance del delincuente, pero también proporcionaban poderosas herramientas de investigación a los poderes públicos. Surgía así la necesidad de encontrar un delicado equilibrio entre la capacidad del Estado para hacer frente a un fenómeno criminal de nuevo cuño y el espacio de exclusión que nuestro sistema constitucional garantiza a cada ciudadano frente a terceros[730].

[728] Publicada en el Boletín Oficial del Estado de 31 de marzo de 2015.

[729] *Vid*. Preámbulo de dicha Ley Orgánica.

[730] El apartado IV de la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. ***"****Por muy meritorio que haya sido el esfuerzo de jueces y tribunales para definir los límites del Estado en la investigación del delito, el abandono a la creación jurisprudencial de lo que ha de ser objeto de regulación legislativa ha propiciado un déficit en la calidad democrática de nuestro sistema procesal, carencia que tanto la dogmática como instancias supranacionales han recordado. El Tribunal Constitucional ha apuntado el carácter inaplazable de una regulación que aborde las intromisiones en la privacidad del investigado en un proceso penal. Hoy por hoy, carecen de cobertura y su subsanación no puede obtenerse acudiendo a un voluntarista expediente de integración analógica que desbordaos límites de lo constitucionalmente aceptable. Solo así se podrá evitar la incidencia negativa que el actual estado de cosas está proyectando en relación con algunos de los derechos constitucionales que pueden ser objeto de limitación en el proceso penal.*

La necesidad de afrontar de inmediato ciertas cuestiones relacionadas con las nuevas tecnologías propició que se dictara la *Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.* Entre dichas cuestiones se encuentra la regulación de las medidas de investigación tecnológica en el ámbito de los derechos a la intimidad, al secreto de las comunicaciones y a la protección de datos personales garantizados por la Constitución.

Las reformas introducidas en esta materia por la Ley Orgánica 13/2015, son las siguientes:

Se da nueva redacción al Título VIII del Libro II de la Ley de Enjuiciamiento Criminal, cuyo contenido bajo la rúbrica "*De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución"*, es ampliamente desarrollado a través de la introducción de varios capítulos nuevos sobre estas cuestiones:

1) Interceptación de las comunicaciones telefónicas y telemáticas (Capitulo V).

2) Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos (Capítulo VI).

3) Utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización (Capítulo VII).

4) Registro de dispositivos de almacenamiento masivo de información (Capítulo VIII).

5) Registros remotos sobre equipos informáticos (IX).

A todos ellos, le resulta de aplicación el Capítulo IV, relativo a las disposiciones comunes a la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de

información y los registros remotos sobre equipos informáticos y como medida de aseguramiento la Orden de Conservación de Datos (Capítulo X).

Se da nueva redacción a la a detención y apertura de la correspondencia escrita y telegráfica en un nuevo artículo 579 y se regulan los hallazgos casuales en el artículo 579 bis (Dentro del Capítulo III del Título VIII). Culmina la reforma con una nueva regulación de la figura del agente encubierto, que otorga a éste la posibilidad de usar las nuevas tecnologías en el artículo 282.7 y crea *ex novo* agente encubierto informático en el artículo 282.6.

3.3 La Ley 25/2007, De 18 De Octubre, de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones[731].

A través de esta ley, según se destaca en su Exposición de Motivos, se llevó a efecto la transposición en nuestro ordenamiento jurídico de la *Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo sobre conservación de datos generados y tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes publicas de comunicaciones*. Directiva que fue declarada inválida el 8 abril 2014, por el Tribunal de Justicia de la Unión Europea. Fundamenta dicha invalidez[732], no porque no fuera posible guardar esos datos en ficheros, sino porque entiende el TJUE que conforme al contenido de la Directiva no quedaba suficientemente garantizados los derechos fundamentales de los artículos 7 (derecho a la vida privada y de las comunicaciones) y 8 (protección de los datos de carácter personal) de la Carta de los Derechos de la Unión[733].

---

[731] Se ha dejado constancia, en el epígrafe dedicado a la normativa europea, que fue dictada en transposición de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006 (declarada inválida el 8 abril 2014, por el Tribunal de Justicia de la Unión Europea),sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modificó la Directiva 2002/58/CE.

[732] ENCINAR DEL POZO, M. A. "La invalidez de la Directiva sobre Conservación y Cesión de los Datos relativos a las Comunicaciones". Revista SEPIN SP/DOCT/18682, 7 de noviembre de 2014.

[733] VAZQUEZ SECO, LUIS. Incorporación de datos al proceso. ob. cit pag. 5. Destaca los siguientes pronunciamentos de la Sentencia:
La Directiva constituye una injerencia de gran magnitud y especial gravedad en los derechos fundamentales la intimidad y respeto de la vida privada (apreciados en su conjunto los datos conservados pueden proporcionar indicaciones muy precisas sobre la vida privada de las personas, como los hábitos de

También se han planteado cuestiones prejudiciales ante el Tribunal de Justicia de la Unión por parte de tribunales Británicos y Suecos, actualmente en trámite en los asuntos acumulados C - 203/15 Tele2 Sverige AB/ Post - och telestyrelsen y C - 698/15 Secretary of State for Home Department/ Tom Watson y otros, pendientes de que el Tribunal de Justicia dicte sentencia[734].

---

la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, las relaciones sociales y los medios sociales frecuentados ... es decir, se puede reconstruir y averiguar parte de su vida pasada) y a la protección de datos de carácter personal (la obligación de conservar de forma preventiva y ceder posteriormente deja sin efecto las facultades de consentimiento para la conservación/cesión, información sobre el tratamiento y su finalidad, derechos de acceso, rectificación, oposición y cancelación) recogidos en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea, suponiendo una clara limitación de su contenido.

Tal injerencia responde sin embargo a un fin de interés general, cual es que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro, especialmente contra la delincuencia organizada y el terrorismo.

Tales limitaciones deben cumplir con las exigencias del artículo 52 , apartado 1, de la Carta: cualquier limitación del ejercicio de los derechos y libertades reconocidos por ésta deberá ser establecida por la ley, respetar su contenido esencial y, dentro del respeto del principio de proporcionalidad, sólo podrán introducirse limitaciones a dichos derechos y libertades cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás.

Las condiciones para la limitación de los derechos fundamentales afectados se establecen en la Directiva de forma genérica, sin recoger de forma concreta los supuestos de cesión (en especial, ante qué tipos de delitos se puede autorizar), ni la obligación de que un juez autorice la medida, no establece un plazo de conservación estricto, ni distingue entre categorías de datos a preservar, ni medidas de seguridad suficientes para garantizar que los datos retenidos no sean utilizados para finalidades diferentes, ni una autoridad independiente que vele sobre la aplicación de tales medidas. Por tanto, tales reproches afectan a los principios de proporcionalidad y necesidad en la regulación, ya que el nivel de detalle a la hora de fijar límites precisos y objetivos que hagan la medida compatible con el respecto a los derechos fundamentales afectados no es suficiente para evitar abusos tanto por parte de las autoridades nacionales llamadas a utilizar dichos datos para fines de preservar la seguridad de sus ciudadanos ante la delincuencia grave como el acceso de terceras personas por la no exigencia de medidas de seguridad nítidas.

Al no establecer la obligación de que los datos se conserven en el territorio de la Unión, la Directiva no garantiza el control del cumplimiento de los requisitos de protección y de seguridad por una autoridad independiente, como se exige expresamente en la Carta.

[734] http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62015CC0203. Se ha pronunciado el Abogado General en sus conclusiones de fecha 19 de julio de 2016 en el sentido siguiente:

- La obligación de conservación impuestas por los Estados miembros está incluida en el ámbito de aplicación del artículo 15 de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.
- Los Estados miembros pueden hacer uso de la facultad de establecer mediante una norma interna la obligación de conservar los datos al amparo de la habilitación otorgada por la Directiva 2002/58/CE, pero supeditado a que se cumplan estrictamente los requisitos establecidos no sólo en dicha disposición, sino también de las disposiciones pertinentes de la Carta interpretadas según los dictados contenidos en la sentencia Digital Rights Ireland.

La obligación de conservar/ceder los datos impuesta por la legislación interna de los Estados debe cumplir con los siguientes requisitos para ser compatible con el Derecho de la Unión:

1.- Debe de estar autorizada por una ley.

Nuestro legislador entiende que la Ley española 25/2007 ha ido más allá de la Directiva invalidada 2006/24/CE[735] en la protección y control de los derechos a la privacidad y al secreto de las comunicaciones, pues quedan garantizados en su regulación y por ello se mantiene su eficacia[736], si bien se reformaron ciertos aspectos en la Ley General de Telecomunicaciones 9/2014[737], (posterior a la Sentencia del TJUE) y se estableció expresamente en la reforma de la LECrim que la cesión de datos se rige por lo establecido en la Ley 25/2007, de 18 de octubre.

2.- Debe respetar el contenido esencial de los derechos consagrados por la Carta (tal previsión se cumple cuando se implementan medidas de seguridad contra los riesgos de abuso y contra cualquier acceso o utilización ilícitos respecto de tales datos).
3.- Debe perseguir un objetivo de interés general (la lucha contra los delitos graves constituye una finalidad susceptible de justificar una obligación general de conservar datos, a diferencia de la lucha contra delitos simples o el buen desarrollo de procedimientos no penales)
4.- Debe ser apropiada para la consecución de dicho objetivo (la anterior exigencia no debe de ponerse en relación con la gravedad del delito, sino con la existencia de ciertas garantías con respecto a la forma de acceso a los datos, al período de conservación, así como a la protección y la seguridad de los datos).
5.- Debe ser necesaria para la consecución de dicho objetivo (esta obligación debe llevar aparejadas todas las garantías enunciadas por el Tribunal de Justicia en los apartados 60 a 68 de la sentencia de 8 de abril de 2014, Digital Rights Ireland y otros en relación con el acceso a los datos, el período de conservación, así como la protección y la seguridad de los datos, con el fin de limitar a lo estrictamente necesario el menoscabo a los derechos reconocidos por la Directiva 2002/58 y por los artículos 7 (respeto de la vida privada y familiar :Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones) y 8 (Protección de datos de carácter personal :1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación. 3. El respeto de estas normas estará sujeto al control de una autoridad independiente) de la Carta de Derechos Fundamentales de la Unión Europea.
6.-Debe ser proporcionada, en una sociedad democrática, para la consecución de ese mismo objetivo (ponderar, por una parte, las ventajas que resultan de esta medida en relación con el objetivo legítimo perseguido, y, por otra parte, las desventajas que se derivan de la misma en relación con derechos fundamentales consagrados en una sociedad democrática).

[735]RODRÍGUEZ LAINZ, J L. "Sobre la incidencia de la declaración de invalidez de la Directiva 2006/24/CE en la ley española sobre conservación de datos relativos a las comunicaciones". Diario La Ley nº 8308, Sección Doctrina, 12 de Mayo de 2014. Sostiene que la legislación española sí garantiza dichos estándares de protección y seguridad de los datos conservados por mandato de la Ley 25/2007.

[736] ENCINAR DEL POZO, M.A. "La invalidez de la Directiva sobre Conservación (…)". ob. cit. pág. 15 Opinión no compartida por el autor que sostiene que la Ley 25/2007, de 18 de octubre, no cumple los límites que exige el respeto del principio de proporcionalidad, en relación con los arts. 7, 8 y 52.1 de la Carta. Es decir, la Ley es inválida en la medida en que lo es la Directiva, porque ambas son contrarias a la Carta de Derechos Fundamentales de la Unión Europea.

[737] La Ley 9/2014, de 9 de mayo (BOE 10 de mayo), General de Telecomunicaciones, en su artículo 42 relativo a la conservación y cesión de datos de las comunicaciones electrónicas y redes públicas de comunicaciones, señala que:
"La conservación y cesión de datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación a los agentes facultados a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en leyes especiales se rige por lo establecido en la Ley 25/2007, de 18 de octubre".

La Ley, según el preámbulo de la misma, es respetuosa con los pronunciamientos que, en relación con el derecho al secreto de las comunicaciones, ha venido emitiendo el Tribunal Constitucional, respeto que, especialmente, se articula a través de dos garantías: en primer lugar, que los datos sobre los que se establece la obligación de conservación son datos exclusivamente vinculados a la comunicación, ya sea telefónica o efectuada a través de Internet, pero en ningún caso reveladores del contenido de ésta; y, en segundo lugar, que la cesión de tales datos que afecten a una comunicación o comunicaciones concretas, exigirá, siempre, la autorización judicial previa"[738]. El artículo 1º de citada Ley 25/2007 de 18 de octubre señala que su objeto "*es la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de* dichos *datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código penal o en leyes penales especiales"*.

Del preámbulo de la Ley y del articulado de la misma se puede resumir:

[738] GONZÁLEZ LÓPEZ, J J. "Comentarios a la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones". Revista general de derecho procesal nº 16, 2008. pág 8 y 9. Ambas garantías son, sin embargo, inadecuadas desde la óptica del derecho al secreto de las comunicaciones. Por lo que se refiere a la primera, es uniforme la jurisprudencia del Tribunal Constitucional y del Tribunal Supremo que sostiene que los "datos de tráfico" se hallan incluidos en el ámbito de cobertura del derecho al secreto de las comunicaciones, de manera que las medidas que les afecten supondrán, en principio, restricción del derecho, siempre que operen sobre la comunicación en curso. A igual conclusión se llega en relación con los datos de localización. En cuanto a los de abonado, estos datos en ningún caso corresponden al ámbito de cobertura del derecho, por lo que la supuesta garantía no es tal, sino que simplemente ni siquiera concurre la posibilidad de limitar el derecho al secreto de las comunicaciones. Además, cabe plantearse qué tipo de garantía supone esta limitación. ¿Considera el legislador que sólo se restringe el derecho al secreto de las comunicaciones cuando la medida afecta al contenido (material) de la comunicación? Si es así, no acierta a comprenderse por qué menciona como garantía la resolución judicial exigida para proceder a la cesión, a no ser que parta de considerar la conservación y la cesión como dos medidas autónomas, la primera de las cuales puede llevarse a cabo respecto de los datos de las comunicaciones distintos del contenido (material) sin necesidad de habilitación judicial (¿por no ser restrictiva del derecho?, ¿por su menor gravedad lesiva?) y la segunda, no. Si es así, tampoco se entiende que en la Disposición Adicional Única se admita la cesión de datos que encajan en la categoría de vinculados a las comunicaciones electrónicas distintos del contenido sin reclamar resolución judicial habilitante.
Por lo que respecta a la segunda, la exigencia de "autorización" judicial para la cesión, que, adelantamos, nos parece del todo adecuada, no puede derivarse de la exigencia de resolución judicial del artículo 18.3 CE, ya que la cesión se lleva a cabo una vez concluida la comunicación, esto es, al margen de la cobertura temporal del derecho al secreto de las comunicaciones.
En definitiva, la LCD parte de una concepción claramente errónea de la delimitación del derecho al secreto de las comunicaciones, a partir de la cual llega a conclusiones adecuadas desde el punto de vista del derecho fundamental realmente afectado (el derecho a la protección de los datos de carácter personal) pero que, precisamente debido a su inadecuada fundamentación dogmática, son susceptibles de desdibujar la protección debida a ambos derechos, de lo que hay sobradas muestras en la propia LCD.

- Los sujetos que quedan obligados a conservar[739] los datos, son los operadores que presten sus servicios de comunicaciones electrónicas disponibles al público, o que exploten una red pública de comunicaciones electrónicas en el Territorio Nacional[740]
- los datos a retener: los necesarios para la identificación del origen y el destino de la comunicación, la identidad de los usuarios o abonados, los que permitan determinar el momento y la duración de la comunicación determinada, el tipo de comunicación, los datos necesarios para identificar el equipo de comunicación empleado y en caso de utilización de un equipo móvil, los datos necesarios para su localización La Ley enumera en su art. 3, de manera precisa y detallada, este listado de datos que quedan sujetos a la obligación de conservación en el marco de las comunicaciones por telefonía fija, móvil o Internet[741]. En ningún caso, datos reveladores del contenido de las comunicaciones, ya sea telefónica o efectuada a través de Internet.

---

[739] GONZÁLEZ LÓPEZ, J J. "Comentarios a la Ley 25/2007, de 18 de octubre (…)" ob. cit. pág. 3 "La obligación de conservar determinadas categorías de datos relativos a las comunicaciones electrónicas que la Ley prevé corresponde a la medida que se ha denominado de "retención de datos", tal y como se ha configurado en el marco comunitario, esto es, como la conservación generalizada de datos ya tratados, frente a la "retención" (en el sentido que le atribuye el Consejo de Europa en el CCib) como obtención en tiempo real de ciertas categorías de datos, *y la "preservación", como conservación particularizada de datos ya tratados. En este sentido, la Exposición de Motivos identifica como objeto de la LCD "la obligación de los operadores de telecomunicaciones de retener determinados datos generados o tratados por los mismos, con el fin de posibilitar que dispongan de ellos los agentes facultados", si bien en el artículo 1.1 (dedicado a fijar el objeto de la Ley) se utiliza el término "conservar", aunque también referido a una conservación generalizada.*

[740] El artículo 2º de citada Ley 25/2007 de 18 de octubre señala que "*Son destinatarios de las obligaciones relativas a la conservación de datos impuestas en esta Ley los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones, en los términos establecidos en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones*." Las referencias a la Ley General de Telecomunicaciones se entienden hechas a la Ley 9/2014, de 9 de mayo (BOE 10 de mayo), General de Telecomunicaciones.

[741] Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
Artículo 3 Datos objeto de conservación
1. Los datos que deben conservarse por los operadores especificados en el artículo 2 de esta Ley, son los siguientes:
a) Datos necesarios para rastrear e identificar el origen de una comunicación:
1.° Con respecto a la telefonía de red fija y a la telefonía móvil:
i) Número de teléfono de llamada.
ii) Nombre y dirección del abonado o usuario registrado.
2.° Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:
i) La identificación de usuario asignada.
ii) La identificación de usuario y el número de teléfono asignados a toda comunicación que acceda a la red pública de telefonía.

- La obligación de conservación cesa a los doce meses, ampliable a dos años o reducible a seis meses reglamentariamente[742].

---

iii) El nombre y dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo de Internet (IP), una identificación de usuario o un número de teléfono.
b) Datos necesarios para identificar el destino de una comunicación:
1.º Con respecto a la telefonía de red fija y a la telefonía móvil:
i) El número o números marcados (el número o números de teléfono de destino) y, en aquellos casos en que intervengan otros servicios, como el desvío o la transferencia de llamadas, el número o números hacia los que se transfieren las llamadas.
ii) Los nombres y las direcciones de los abonados o usuarios registrados.
2.º Con respecto al correo electrónico por Internet y la telefonía por Internet:
i) La identificación de usuario o el número de teléfono del destinatario o de los destinatarios de una llamada telefónica por Internet.
ii) Los nombres y direcciones de los abonados o usuarios registrados y la identificación de usuario del destinatario de la comunicación.
c) Datos necesarios para determinar la fecha, hora y duración de una comunicación:
1.° Con respecto a la telefonía de red fija y a la telefonía móvil: la fecha y hora del comienzo y fin de la llamada o, en su caso, del servicio de mensajería o del servicio multimedia.
2.° Con respecto al acceso a Internet, al correo electrónico por Internet y a la telefonía por Internet:
i) La fecha y hora de la conexión y desconexión del servicio de acceso a Internet registradas, basadas en un determinado huso horario, así como la dirección del Protocolo Internet, ya sea dinámica o estática, asignada por el proveedor de acceso a Internet a una comunicación, y la identificación de usuario o del abonado o del usuario registrado.
ii) La fecha y hora de la conexión y desconexión del servicio de correo electrónico por Internet o del servicio de telefonía por Internet, basadas en un determinado huso horario.
d) Datos necesarios para identificar el tipo de comunicación.
1.° Con respecto a la telefonía de red fija y a la telefonía móvil: el servicio telefónico utilizado: tipo de llamada (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluido el reenvío o transferencia de llamadas) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia avanzados y servicios multimedia).
2.° Con respecto al correo electrónico por Internet y a la telefonía por Internet: el servicio de Internet utilizado.
e) Datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación:
1.º Con respecto a la telefonía de red fija: los números de teléfono de origen y de destino.
2.° Con respecto a la telefonía móvil:
i) Los números de teléfono de origen y destino.
ii) La identidad internacional del abonado móvil (IMSI) de la parte que efectúa la llamada.
iii) La identidad internacional del equipo móvil (IMEI) de la parte que efectúa la llamada.
iv) La IMSI de la parte que recibe la llamada.
v) La IMEI de la parte que recibe la llamada.
vi) En el caso de los servicios anónimos de pago por adelantado, tales como los servicios con tarjetas prepago, fecha y hora de la primera activación del servicio y la etiqueta de localización (el identificador de celda) desde la que se haya activado el servicio.
3.° Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:
i) El número de teléfono de origen en caso de acceso mediante marcado de números.
ii) La línea digital de abonado (DSL) u otro punto terminal identificador del autor de la comunicación.
f) Datos necesarios para identificar la localización del equipo de comunicación móvil:
1.° La etiqueta de localización (identificador de celda) al inicio de la comunicación.
2.° Los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el período en el que se conservan los datos de las comunicaciones.
2. Ningún dato que revele el contenido de la comunicación podrá conservarse en virtud de esta Ley.

[742] Artículo 5 de la ley "1. *La obligación de conservación de datos impuesta cesa a los doce meses computados desde la fecha en que se haya producido la comunicación. Reglamentariamente, previa consulta a los operadores, se podrá ampliar o reducir el plazo de conservación para determinados datos o una categoría de datos hasta un máximo de dos años o un mínimo de seis meses, tomando en*

- La cesión[743] de la información se efectuará mediante formato electrónico a los agentes facultados, que según el artículo 6 de la ley, son:

a) Los miembros de las Fuerzas y Cuerpos de Seguridad, cuando desempeñen funciones de policía judicial, de acuerdo con lo previsto en el artículo 547 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

b) Los funcionarios de la Dirección Adjunta de Vigi- lancia Aduanera, en el desarrollo de sus competencias como policía judicial, de acuerdo con el apartado 1 del artículo 283 de la Ley de Enjuiciamiento Criminal.

c) El personal del Centro Nacional de Inteligencia en el curso de las investigaciones de seguridad sobre personas o entidades, de acuerdo con lo previsto en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia.

- Exigencia en todo caso de autorización judicial previa[744].

---

consideración el coste del almacenamiento y conservación de los datos, así como el interés de los mismos para los fines de investigación, detección y enjuiciamiento de un delito grave, previa consulta a los operadores".

[743] GONZÁLEZ LÓPEZ, J J. "Comentarios a la Ley 25/2007, de 18 de octubre (…)". ob.cit. pág. 5. *"Junto a la regulación de la conservación generalizada de datos relativos a las comunicaciones electrónicas, la LCD se ocupa igualmente del procedimiento de cesión de dichos datos, lo cual, si bien resulta necesario a fin de garantizar el propósito mediato de la medida (poner a disposición de las autoridades encargadas de la prevención y persecución de delitos o de la seguridad nacional los datos conservados) afecta a una materia cuyo alcance no se limita a los datos correspondientes a las comunicaciones electrónicas: la cesión de datos de carácter personal como medida orientada a la prevención o persecución penal. El concepto de "detección" no está nada claro, y aunque parece referirse a la utilización de los datos con fines preventivos (por oposición al término "investigación"), no se concreta su alcance 21. Este hecho, del que ya advertimos en relación con el Proyecto de Ley, es particularmente relevante, ya que la idea de "detección" induce a pensar que el hallazgo de delitos será susceptible de efectuarse indiciariamente, esto es, al margen de la existencia de indicios de delito o con apoyo en simples sospechas sin base fáctica suficiente".*

[744] Artículo 7.2. de la *LCD* "*La resolución judicial determinará, conforme a lo previsto en la Ley de Enjuiciamiento Criminal y de acuerdo con los principios de necesidad y proporcionalidad, los datos conservados que han de ser cedidos a los agentes facultados".*

- El plazo de ejecución de la orden de cesión será el fijado por la resolución judicial. Si no se establece otro plazo distinto, la cesión deberá efectuarse dentro del plazo de 7 días naturales[745].
- y deberán estar disponibles y ser cedidos a los fines de detección o investigación por delitos graves.
- Por último, la ley prevé un régimen de responsabilidad a los operadores en el caso de incumplimiento de las obligaciones impuestas en la ley[746] y la medida instrumental consistente en el registro vinculado a las tarjetas de prepago[747].

La Sala General no jurisdiccional aprobó el 23 de febrero de 2010 el siguiente acuerdo*: Es necesaria la autorización judicial para que los operadores que prestan servicios de comunicaciones electrónicos o de redes públicas de comunicación cedan los datos generados o tratados con tal motivo. Por lo cual, el Ministerio Fiscal precisará de tal autorización para obtener de los operadores los datos conservados que se especifican en el art. 3 de la Ley 25/2007 de 18 de octubre ".*

[745] Artículo 7.3 de la LCD.

[746] Artículo 10. LCD. Infracciones y sanciones.
1. Constituyen infracciones a lo previsto en la presente Ley las siguientes:
a) Es infracción muy grave la no conservación en ningún momento de los datos a los que se refiere el artículo 3.
b) Son infracciones graves:
i) La no conservación reiterada o sistemática de los datos a los que se refiere el artículo 3.
ii) La conservación de los datos por un período inferior al establecido en el artículo 5.
iii) El incumplimiento deliberado de las obligaciones de protección y seguridad de los datos establecidas en el artículo 8.
c) Son infracciones leves:
i) La no conservación de los datos a los que se refiere el artículo 3 cuando no se califique como infracción muy grave o grave.
ii) El incumplimiento de las obligaciones de protección y seguridad de los datos establecidas en el artículo 8, cuando no se califique como infracción grave.
2. A las infracciones previstas en el apartado anterior, a excepción de las indicadas en los apartados 1.b).iii y 1.c).ii de este artículo, les será de aplicación el régimen sancionador establecido en la Ley General de Telecomunicaciones, correspondiendo la competencia sancionadora al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información, sin perjuicio de las responsabilidades penales que pudieran derivar del incumplimiento de la obligación de cesión de datos a los agentes facultados.
El procedimiento para sancionar las citadas infracciones se iniciará por acuerdo del Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información, pudiendo el Ministerio del Interior instar dicho inicio.
En todo caso, se deberá recabar del Ministerio del Interior informe preceptivo y determinante para la resolución del procedimiento sancionador.
3. A las infracciones previstas en los apartados 1.b).iii y 1.c).ii de este artículo les será de aplicación el régimen sancionador establecido en la Ley General de Telecomunicaciones, correspondiendo la competencia sancionadora a la Agencia Española de Protección de Datos.

[747] GONZÁLEZ LÓPEZ, J J. "Comentarios a la Ley 25/2007, de 18 de octubre(…)" ob. cit. pág. 28 la previsión de que los operadores de servicios de telefonía móvil que comercialicen servicios con sistema de activación mediante la modalidad de tarjetas de prepago deberán llevar un libro-registro en que conste la identidad de los clientes que adquieran una tarjeta con dicha modalidad de pago constituye una medida instrumental respecto de la conservación generalizada de datos, destinada a paliar una de las dificultades

Esta medida estaba limitada a los delitos graves, con fundamento, en la supuesta restricción del derecho al secreto de las comunicaciones y a la necesidad de paliar, de alguna manera, la gravedad de la restricción que implicaba la conservación generalizada a que va ligada la cesión, pero no tenía en cuenta que la afección a datos distintos del contenido material de la comunicación (a la que sorprendentemente alude la Exposición de Motivos como garantía asociada al derecho al secreto de las comunicaciones, sin atender el hecho de que justamente en el ámbito del principio de proporcionalidad dicha delimitación resulta relevante) podría justificar, incluso desde la perspectiva del derecho al secreto de las comunicaciones la afección practicada con el fin de investigar delitos no necesariamente graves, aunque sí cualificados, en el sentido indicado.

El Pleno de la Sala de lo Penal del Tribunal Supremo, de fecha 20 de enero de 2010 sobre la interpretación de la ley 25/2007 de conservación de datos en relación con la ley orgánica de protección de datos, sostenía que la obtención de datos a la que se refiere la Ley 25/2007, era un medio de investigación necesario, dada la complejidad de los delitos que se cometían a través de internet, que de otra manera cerraría la instrucción de numerosos hechos delictivos, al no poderse averiguar la identidad de los presuntos responsables por otros medios tradicionales de investigación. Pero de aplicar una interpretación literal, y conforme al espíritu de la ley, solo podría adoptarse cuando se investigaran delitos graves conforme a nuestra legislación, es decir, aquellos que conforme al Código Penal estaban sancionados con pena de prisión superior a cinco años.

La reforma de la Ley de Enjuiciamiento Criminal, operada por *Ley Orgánica 13/2015, de 5 de octubre,* solucionó esta cuestión, al no hacer referencia a la gravedad de delito y sino que se autoriza cuando se trate de la investigación de un delito que, por razones vinculadas al principio de proporcionalidad, sea de los que justifican el sacrificio de la inviolabilidad de las comunicaciones. Esto es, podrá ser concedida cuando el conocimiento de esos datos resulte indispensable para la investigación, que tenga ésta además por objeto alguno de los delitos a que se refiere el artículo 579.1 LECrim (*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*

---

que cuestionan la eficacia de este tipo de medidas: la "anonimización" de los usuarios de las comunicaciones electrónicas.

de terrorismo) o delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación.

No obstante, está pendiente que el Tribunal de Justicia de la Unión Europea se pronuncie sobre la cuestión prejudicial planteada por la Sección Cuarta de la Audiencia de Tarragona mediante auto de 6 de abril de 2016, en relación a sí el procedimiento de cesión de datos introducido en reforma de LO 13/2015, al no limitar la cesión a la gravedad del delito, es compatible con las exigencias contenidas en la sentencia de 8 de abril de 2014 que anuló la Directiva 2006/24/CE.

3.4 La Ley 9/2014, de 9 de mayo (BOE 10 de mayo), General de Telecomunicaciones.

Mención aparte dentro de nuestra legislación merece la Ley 9/2014, de 9 de mayo (BOE 10 de mayo), General de Telecomunicaciones que sustituye a la antigua Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, pues establece la protección no penal del secreto de las telecomunicaciones y de los datos personales en el sector[748]. Dentro de su articulado se dedican diversos preceptos a cuestiones procesales, en concreto, bajo la rúbrica de "secreto de las comunicaciones", el capítulo III se dedica a regular el *Secreto de las comunicaciones y protección de los datos personales y derechos y obligaciones de carácter público vinculados con las redes y servicios de comunicaciones electrónicas.*

El artículo 39 dedicado a la interceptación de las comunicaciones[749] establece la obligación a los operadores que exploten redes públicas de comunicaciones electrónicas

[748] ROMEO CASABONA, C. M. *La protección penal de los mensajes de correo electrónico y de otras comunicaciones de carácter personal a través de internet.* en "Derecho y conocimiento"*, vol. 2,* Facultad de Derecho. Universidad de Huelva, pags. 123-149.

[749] La Disposición Final Primera de la Ley de Conservación de Datos dio nueva redacción al artículo 33 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, en el que, bajo la rúbrica de "secreto de las comunicaciones", señalaba que los operadores estaban obligados a realizar las interceptaciones que se autorizasen de acuerdo con lo dispuesto en el artículo 579 de la Ley de Enjuiciamiento Criminal; y se añadía que los sujetos obligados debían facilitar al agente facultado los datos indicados en la orden de interceptación legal, indicando que la identidad o identidades del sujeto objeto de la medida de interceptación sería uno de esos datos a facilitar, así como la identidad o identidades de otras personas involucradas en la comunicación electrónica. Es de notar que ese artículo 33 de la Ley 32/2003 no hacia referencia alguna a la gravedad del delito que se investigaba, y se limitaba a remitirse a lo dispuesto en el artículo 579 de la Ley de Enjuiciamiento Criminal. Tras la derogación de la

o que presten servicios de comunicaciones electrónicas disponibles al público, de garantizar el secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias, y de realizar las interceptaciones que se autoricen de acuerdo con lo establecido en el Título VIII del Libro II de la LECrim bajo el título "*de las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución*" (antiguo artículo 579 de la Ley de Enjuiciamiento Criminal)[750], en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia y en otras normas con rango de Ley Orgánica. Asimismo, deberán adoptar a su costa las medidas que se establecen en este artículo y en los reglamentos correspondientes.

Esta interceptación deberá facilitarse para cualquier comunicación que tenga como origen o destino el punto de terminación de red o el terminal específico que se determine a partir de la orden de interceptación legal, incluso aunque esté destinada a dispositivo de almacenamiento o procesamiento de la información; asimismo, la interceptación podrá realizarse sobre un terminal conocido y con unos datos de ubicación temporal para comunicaciones desde locales públicos. Cuando no exista una vinculación fija entre el sujeto de la interceptación y el terminal utilizado, éste podrá ser determinado dinámicamente cuando el sujeto de la interceptación lo active para la comunicación mediante un código de identificación personal. El acceso se facilitará para todo tipo de comunicaciones electrónicas, en particular, por su penetración y cobertura, para las que se realicen mediante cualquier modalidad de los servicios de telefonía y de transmisión de datos, se trate de comunicaciones de vídeo, audio, intercambio de mensajes, ficheros o de la transmisión de facsímiles. El acceso facilitado servirá tanto para la supervisión como para la transmisión a los centros de recepción de las interceptaciones de la comunicación electrónica interceptada y la información

antigua Ley de comunicaciones por la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, el contenido de ese precepto se mantiene en el artículo 39 de esta última, hoy vigente.

[750] La Disposición adicional segunda de la Ley Orgánica *13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.*
Sustitución de referencias.
"Las disposiciones contenidas en otros textos legales que se refieran a la intervención de las comunicaciones telefónicas o telemáticas previstas en el artículo 579 de la Ley de Enjuiciamiento Criminal se tendrán por referenciadas a lo dispuesto en el Título VIII del Libro II de dicha ley".

relativa a la interceptación, y permitirá obtener la señal con la que se realiza la comunicación.

Los sujetos obligados[751] deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición, los datos indicados en la orden de interceptación legal, de entre los que se relacionan a continuación:

a) Identidad o identidades del sujeto objeto de la medida de la interceptación.

Se entiende por identidad: etiqueta técnica que puede representar el origen o el destino de cualquier tráfico de comunicaciones electrónicas, en general identificada mediante un número de identidad de comunicaciones electrónicas físico (tal como un número de teléfono) o un código de identidad de comunicaciones electrónicas lógico o virtual (tal como un número personal) que el abonado puede asignar a un acceso físico caso a caso.

b) Identidad o identidades de las otras partes involucradas en la comunicación electrónica.

c) Servicios básicos utilizados.

d) Servicios suplementarios utilizados.

e) Dirección de la comunicación.

f) Indicación de respuesta.

g) Causa de finalización.

h) Marcas temporales.

i) Información de localización.

j) Información intercambiada a través del canal de control o señalización.

[751] Art. 39.8 "*Los sujetos obligados deberán facilitar al agente facultado, de entre los datos previstos en los apartados 5, 6 y 7 de este artículo, sólo aquéllos que estén incluidos en la orden de interceptación legal"*.

De las otras partes que intervengan en la comunicación que sean clientes del sujeto obligado, los siguientes datos:

a) Identificación de la persona física o jurídica.

b) Domicilio en el que el proveedor realiza las notificaciones.

Y, aunque no sea abonado, si el servicio de que se trata permite disponer de alguno de los siguientes:

c) Número de titular de servicio (tanto el número de directorio como todas las identificaciones de comunicaciones electrónicas del abonado).

d) Número de identificación del terminal.

e) Número de cuenta asignada por el proveedor de servicios Internet.

f) Dirección de correo electrónico.

También deberán facilitar información acerca de la situación geográfica del terminal o punto de terminación de red origen de la llamada, y de la del destino de la llamada. En caso de servicios móviles, se proporcionará una posición lo más exacta posible del punto de comunicación y, en todo caso, la identificación, localización y tipo de la estación base afectada.

Con carácter previo a la ejecución de la orden de interceptación legal, los sujetos obligados deberán facilitar al agente facultado información sobre los servicios y características del sistema de telecomunicación que utilizan los sujetos objeto de la medida de la interceptación y, si obran en su poder, los correspondientes nombres de los abonados con sus números de documento nacional de identidad, tarjeta de identidad de extranjero o pasaporte, en el caso de personas físicas, o denominación y código de identificación fiscal en el caso de personas jurídicas.

Los sujetos obligados deberán tener en todo momento preparadas una o más interfaces a través de las cuales las comunicaciones electrónicas interceptadas y la información relativa a la interceptación se transmitirán a los centros de recepción de las interceptaciones. Las características de estas interfaces y el formato para la transmisión

de las comunicaciones interceptadas a estos centros estarán sujetas a las especificaciones técnicas que se establezcan por el Ministerio de Industria, Energía y Turismo.

Por último, en el caso de que los sujetos obligados apliquen a las comunicaciones objeto de interceptación legal algún procedimiento de compresión, cifrado, digitalización o cualquier otro tipo de codificación, deberán entregar aquellas desprovistas de los efectos de tales procedimientos, siempre que sean reversibles. Las comunicaciones interceptadas deben proveerse al centro de recepción de las interceptaciones con una calidad no inferior a la que obtiene el destinatario de la comunicación.

El artículo 40 es dedicado a la interceptación de las comunicaciones electrónicas por los servicios técnicos.

1. Con pleno respeto al derecho al secreto de las comunicaciones y a la exigencia, conforme a lo establecido en la Ley de Enjuiciamiento Criminal, de autorización judicial para la interceptación de contenidos, cuando para la realización de las tareas de control para la eficaz utilización del dominio público radioeléctrico o para la localización de interferencias perjudiciales sea necesaria la utilización de equipos, infraestructuras e instalaciones técnicas de interceptación de señales no dirigidas al público en general, será de aplicación lo siguiente:

a) La Administración de las telecomunicaciones deberá diseñar y establecer sus sistemas técnicos de interceptación de señales en forma tal que se reduzca al mínimo el riesgo de afectar a los contenidos de las comunicaciones.

b) Cuando, como consecuencia de las interceptaciones técnicas efectuadas, quede constancia de los contenidos, los soportes en los que éstos aparezcan deberán ser custodiados hasta la finalización, en su caso, del expediente sancionador que hubiera lugar o, en otro caso, destruidos inmediatamente. En ninguna circunstancia podrán ser objeto de divulgación.

2. Las mismas reglas se aplicarán para la vigilancia del adecuado empleo de las redes y la correcta prestación de los servicios de comunicaciones electrónicas.

3. Lo establecido en este artículo se entiende sin perjuicio de las facultades que a la Administración atribuye el artículo 60.

El artículo 42 sostiene que la conservación y cesión de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones que se regulará por ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

El artículo 43 permite el cifrado en las redes y servicios de comunicaciones electrónicas, como instrumento en la seguridad de la información aunque se establece la obligación de facilitar a un órgano de la Administración General del Estado o a un organismo público, los algoritmos o cualquier procedimiento de cifrado utilizado.

Por último, la Ley en su artículo 41 impone a los operadores la obligación de garantizar los datos de carácter personal y de establecer una serie de medidas para tal fin, así como garantizar la integridad y seguridad de las redes y de los servicios de comunicaciones electrónicas.

3.5 La Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal.[752]

Las obligaciones relativas a las medidas para garantizar la calidad de los datos y la confidencialidad y seguridad en el tratamiento de los mismos son las establecidas en la Ley Orgánica 15/1999 de 13 de diciembre y su normativa de desarrollo. Esta ley supuso una modificación importante del régimen sobre protección de datos, y tiene como objetivo "garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar[753].

[752] Reglamento de desarrollo, Real Decreto 1720/2007 de 21 de diciembre, que entró en vigor el 31 de marzo de 2008 .

[753] Artículo 2 de la LO 15/1999

" 1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:

a. Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.

El nivel de protección de los datos almacenados se determinará de conformidad con lo previsto en la Ley Orgánica 15/1999 de 13 de diciembre, de tal modo que sin el consentimiento de su titular, unos datos reservados contenidos en archivos informáticos, no pueden facilitarse a nadie, salvo los casos especiales que autorizan sus propias normas, entre las que se halla la autorización judicial, que lógicamente estaría justificada en un proceso de investigación penal[754].

Se regula el régimen jurídico del acceso a los ficheros de tal modo que es conveniente resaltar que 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 están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad (artículo 22.2).

---

b. Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.

c. Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

2. El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación:

a. A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

b. A los ficheros sometidos a la normativa sobre protección de materias clasificadas.

c. A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia Española de Protección de Datos.

3. Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:

a. Los ficheros regulados por la legislación de régimen electoral. Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.

b. Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas.

c. Los derivados del Registro Civil y del Registro Central de penados y rebeldes.

d. Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.

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

Además, "la recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos", a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio, del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales" (artículo 22.3).

Esa capacidad de recogida de datos que esta otorga a las Fuerzas y Cuerpos de Seguridad del Estado, no puede, desde luego, servir de excusa para la creación de un régimen incontrolado de excepcionalidad a su favor. Pero tampoco cabe desconocer que la recogida de ese dato en el marco de una investigación criminal -nunca con carácter puramente exploratorio-, para el esclarecimiento de un delito de especial gravedad, puede reputarse proporcionada, necesaria y, por tanto, ajena a cualquier vulneración de relieve constitucional.

También parece evidente que esa legitimidad que la Ley confiere a las Fuerzas y Cuerpos de Seguridad del Estado nunca debería operar en relación con datos referidos al contenido del derecho al secreto de las comunicaciones (artículo 18.3 de la Constitución), o respecto de datos susceptibles de protección por la vía del artículo 18.4 de la Constitución que afectarán a lo que ha venido en llamarse el núcleo duro de la privacidad o, con la terminología legal, los datos especialmente protegidos (artículo 7.2 LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal).

APÉNDICE JURISPRUDENCIAL

I. TRIBUNAL EUROPEO DE DERECHOS HUMANOS.

- STEDH de 6 de septiembre de 1978, asunto *Klass* y otros contra Alemania (secreto de las comunicaciones).
- STEDH de 2 de agosto de 1984, caso *Malone* contra Reino Unido (secreto de las comunicaciones, art. 8 CEDH).
- STEDH de15 de junio de 1992, caso Lüdi contra Suiza (secreto de las comunicaciones).
- STEDH de 25 de marzo de 1998, caso *Kopp* contra Suiza (secreto de las comunicaciones).
- STEDH de 30 de julio de 1998, caso Valenzuela Contreras contra España (secreto de las comunicaciones).
- STEDH (Gran Sala) 4 de mayo de 2000, caso *Rotaru* contra Rumanía (art. 8 CEDH).
- STEDH (sección 3ª) 20 de junio de 2000, caso *Foxley* contra Reino Unido (secreto de las comunicaciones).
- STEDH (sección 2ª) 28 de septiembre de 2000, caso *Messina* contra Italia (art. 8 CEDH).
- STEDH (sección 4ª) 18 de febrero de 2003, caso Prado Bugallo contra España (secreto de las comunicaciones).
- Decisión (sección 5ª) 26 de septiembre de 2006, caso Abdulkadir Coban contra España (secreto de las comunicaciones).
- STEDH (Sección 4ª) 3 de abril de 2007, caso *Copland* contra Reino Unido (art. 8 CEDH).
- STEDH (Sección 4ª) 2 diciembre 2008, caso *K.U.* contra Finlandia (art. 8, condena al Estado por no tener normativa que obligue a los ISP a entregar datos para la investigación ciberdelitos)
- STEDH (Sección 1ª) de 3 de julio de 2012, caso *Robathin* contra Austria (art. 8 registro informático).
- STEDH (sección 1ª) de 30 de octubre de 2014, caso *Nosko y Nefedov* contra Rusia (provocación al delito).

- STEDH (Sección 4ª) de 12 de enero de 2016, caso *Szabó y Vissy* contra Hungría (intimidad personal, secreto de las comunicaciones).

II. TRIBUNAL CONSTITUCIONAL.

- STC 114/1984, de 29 de noviembre (secreto de las comunicaciones, revelación por un comunicante, prueba ilícita).
- STC 127/1990 de 5 de julio (pericial en el plenario).
- STC 171/1990, de 12 de noviembre (derecho fundamental a la intimidad).
- STC 24/1991, de 11 de febrero (pericial no ratificada).
- STC 254/1993, de 20 de julio (derecho a la protección de datos).
- STC 303/1993, de 25 de octubre (presunción de inocencia, aplicación inmediata de la jurisprudencia del TEDH).
- STC 85/1994, de 14 de marzo (prueba ilícita, la doctrina de los frutos del árbol envenenado).
- STC 49/1996, 26 de marzo (secreto de las comunicaciones y hallazgo casual)
- STC 54/1996, de 26 de marzo (secreto de las comunicaciones, motivación de las resolución).
- STC 207/1996, de 16 de diciembre (derecho fundamental a la intimidad).
- STC 41/1998, de 24 de febrero (hallazgo casual).
- STC 81/1998, de 2 de abril (prueba ilícita, conexión de antijuricidad).
- STC 94/1998, de 4 de mayo (derecho a la protección de datos).
- STC 49/1999, 5 de abril (secreto de las comunicaciones, motivación).
- STC 144/1999, de 22 de julio (derecho a la protección de datos).
- STC 161/1999, 27 de septiembre (sobre nulidad de la prueba).
- STC 202/1999, de 8 de noviembre (derecho a la protección de datos, "habeas data").
- STC 115/2000, de 5 de mayo (derecho fundamental a la intimidad).
- STC 290/2000, de 30 de noviembre (derecho a la protección de datos).
- STC 70/2001, de 3 de abril (derecho fundamental a la intimidad).
- STC 14/2001, de 29 de enero (intervención telefónica).
- STC 202/2001 de 15 de octubre (secreto de las comunicaciones, motivación de la resolución).

- STC 138/2001, de 18 de junio (secreto de las comunicaciones, requisitos para la injerencia).
- STC 70/2002, 3 de abril (derecho a la intimidad).
- STC 83/2002, de 22 de abril (derecho fundamental a la intimidad).
- STC 123/2002, de 20 de mayo (secreto de las comunicaciones).
- STC 230/2002, de 9 de diciembre (amparo por vulneración del derecho a un proceso con todas las garantías).
- STC 167/2002, de 18 de septiembre (conexión de antijuricidad, motivación de las escuchas).
- STC 14/2003, de 28 de enero (derecho fundamental a la intimidad).
- STC 22/2003, 10 de febrero (prueba ilícita, *deterrent effect*).
- STC 41/2003, de 27 de febrero (amparo por falta de un proceso con todas las garantías).
- STC 56/2003, de 24 de marzo (secreto de las comunicaciones, grabación por un interlocutor).
- STC 170/2003, de 29 de septiembre (registro de ordenadores).
- STC 184/2003, de 23 de octubre (secreto de las comunicaciones, indicios).
- STC 196/2004, de 15 de noviembre (derecho fundamental a la intimidad).
- ATC 400/2004, de 27 de octubre (hallazgo casual intervención de las comunicaciones).
- STC 259/2005, de 24 de octubre (secreto de las comunicaciones, motivación, conexión de antijuricidad).
- STC 26/2006, de 30 de enero (secreto de las comunicaciones)
- STC 89/2006, de 27 de marzo (derecho fundamental a la intimidad).
- STC 104/2006, de 3 de abril (requisitos intervención de comunicaciones).
- STC 136/2006, de 8 de mayo (secreto de las comunicaciones, motivación).
- STC 150/2006, de 22 de mayo (identificación del terminal)
- STC 196/2006, de 3 de julio (derecho fundamental a la intimidad).
- STS 208/2006, de 20 de febrero (legalidad de las grabaciones efectuadas por un interlocutor sin conocimiento de la otra parte).
- STC 253/2006, de 11 de septiembre (derecho fundamental al secreto de las comunicaciones).
- STC 281/2006, de 9 de octubre (secreto de las comunicaciones).
- STC 55/2007, de 12 de marzo (derecho al juez imparcial).

- STC 206/2007, de 24 de septiembre (derecho fundamental a la intimidad, consentimiento).
- ATC 245/2007, de 22 de mayo (intervención telefónica, garantías).
- STC 230/2007, de 5 de noviembre (secreto de las comunicaciones).
- ATC 115/2008, de 28 de abril (sobre peritos de organismos oficiales).
- STC 70/2009, de 23 de marzo (derecho a la intimidad).
- STC 148/2009, de 15 de junio (sobre motivación de la Resoluciones judiciales).
- STC 159/2009, de 29 de junio (derecho fundamental a la intimidad).
- STC 197/2009, de 28 de septiembre (intervención de comunicaciones, indicios).
- STC 219/2009, de 21 de diciembre (derecho fundamental al secreto de las comunicaciones).
- STC 220/2009, de 21 de diciembre (secreto de las comunicaciones, identificación terminal).
- STC 5/2010, de 7 de abril (secreto de las comunicaciones).
- STC 26/2010, de 27 de abril (secreto de las comunicaciones, datos objetivos, introducción de escuchas telefónicas al juicio oral).
- ATC 35/2010, de 9 de marzo (requisitos intervención telefónica).
- STC 70/2010, de 18 de octubre (prueba indiciaria).
- STC 72/2010, de 18 de octubre (motivación por remisión).
- STC 25/2011, 14 de marzo (secreto de las comunicaciones, auto motivado).
- STC 173/2011, de 7 de noviembre (derecho fundamental a la intimidad, derecho al propio entorno virtual).
- STC 142/2012, de 2 de julio (derecho fundamental a la intimidad, acceso a la agenda de un teléfono móvil).
- STC 115/2013, de 9 de mayo (derecho fundamental a la intimidad, distingue entre el acceso a una agenda de un móvil y el acceso al listado de llamadas).
- STC 145/2014, de 22 de septiembre (vulneración del secreto de las comunicaciones por falta de habilitación legal).

III. TRIBUNAL SUPREMO.

- ATS de 18 de junio de 1992 (rec. 610/1990) (sobre intervención telefónica y hallazgo casual).
- STS 22 de enero de 1992 (rec. 846/1989) (prueba aportada por el tribunal art. 729.2 LECrim)
- STS 6 de mayo de 1993 (rec. 2339/1991). (grabación en espacios abiertos).
- STS 25 de junio de 1993 (rec. 2907/1991) (intervención telefónica).
- STS 606/1994, de 18 de marzo (intervención telefónica, identificación del terminal).
- STS 787/1994, de 18 de abril (intervención de teléfono público).
- STS 1038/1994, de 20 de mayo (intervención telefónica doctrina general).
- STS 1579/1994, de 12 de septiembre (requisitos intervención telefónica).
- STS 578/1995, de 28 de abril (hallazgo casual en registro domiciliario).
- STS 768/1995, de 14 de junio (identificación del terminal en la intervención telefónica).
- STS 904/1995, de 23 de septiembre (art. 729.2 LECrim).
- STS 11 de noviembre de 1996 (rec. 113/1996) (pericial sin ratificar).
- STS 914/1996, 20 diciembre (requisitos intervención telefónica).
- STS 792/1997, de 30 de mayo (hallazgo casual).
- STS 805/1997, de 7 de junio (hallazgo casual).
- STS 974/1997, de 4 de julio (prueba ilícita, descubrimiento inevitable con buena fe).
- STS 1149/1997, de 26 de septiembre (hallago casual).
- Sentencia del Tribunal Supremo de 3 de noviembre de 1997, Sala 3ª, (rec. 544/1995) Sobre el documento electrónico.
- STS 465/1998, de 30 de marzo (hallazgo casual).
- STS 467/1998, de 3 de abril (requisitos intervención telefónica, teléfono público).
- STS 622/1998, de 11 de mayo (requisitos intervención telefónica).
- STS 1052/1998, de 21 de septiembre (identificación terminal en la intervención).
- STS 1426/1998, de 23 de noviembre (intervención telefónica).
- STS 93/1999, de 16 de abril (provocación delictiva).

- Acuerdo del Pleno no jurisdiccional de la Sala Segunda de 21 de mayo de 1999.
- STS 960/1999, de 15 de junio (intervención de teléfono de tercera persona no investigada).
- STS 1599/1999, de 15 de noviembre (volcado de datos, pericial informática).
- STS 126/2000, de 16 mayo (intervención telefónica en un delito de hurto).
- STS 316/2000, de 3 de marzo (relativa al conocimiento por los agentes policiales de los listados telefónicos de las agendas de teléfonos móviles).
- STS 1186/2000, de 28 junio (art. 729.2 LECrim).
- STS 1511/2000, de 7 de marzo (peritos oficiales).
- STS1642/2000, de 23 de octubre (informes periciales no ratificados).
- STS 1898/2000, de 12 de diciembre (intervención telefónica).
- Acuerdo del Peno no jurisdiccional de 23 de febrero de 2001 que ratifica el Acuerdo de 21 de mayo de 1999.
- STS 776/2001, de 20 de julio (juicio de fiabilidad).
- STS 832/2001, de 14 de mayo (identificación del investigado en la intervención de comunicaciones).
- STS 833/2001, de 14 de mayo (función de la transcripción de las grabaciones).
- STS 2026/2001, de 28 de noviembre (interceptación de comunicación entre sospechoso y letrado).
- STS 2389/2001, de 14 diciembre (art. 729.2 LECrim).
- STS 543/2002, de 25 de marzo (intervención de teléfono de un no investigado).
- STS 1046/2002, de 3 de junio (intervención telefónica, motivación)
- STS 1235/2002, de 27 de junio (conocimiento por los agentes policiales de las agendas de teléfonos móviles).
- STS 1330/2002, de 16 de julio (intervención telefónica).
- STS 1482/2002, de 17 septiembre (art. 729.2º LECrim).
- STS 262/2003, de 19 de febrero (provocación delictiva)
- STS 277/2003, de 26 de febrero (derecho al juez imparcial).
- STS 315/2003, de 4 de marzo (hallazgo casual, flagrancia).
- STS 587/2003, de 16 de abril (pericial en juicio oral).
- STS 769/2003, de 31 de mayo (protección de datos).

- STS 905/2003, de 18 de junio (comunicante accidental).
- STS 981/2003, de 3 de julio (hallazgo caual).
- STS 988/2003, de 4 de julio (intervención de comunicaciones, requisitos)
- STS 1086/2003 de 25 de julio (conocimiento por los agentes policiales de las agendas de teléfonos móviles).
- STS 1231/2003, de 25 de septiembre (conocimiento por los agentes policiales de las agendas de teléfonos móviles).
- STS 1365/2003, de 17 de octubre (dualidad de peritos).
- STS 1520/2003, de 17 de noviembre (pericial).
- STS 13/2004, de 16 de enero (peritos oficiales).
- STS 182/2004, de 23 de abril (secreto en la intervención de comunicaciones).
- STS 499/2004, de 23 de abril (sobre peritos de la CNMV en delitos económicos).
- STS 530/2004, de 29 de abril (intervención telefónica, requisitos).
- STS 885/2004, de 5 de Julio (hallazgo casual).
- STS 1081/2004, de 30 de septiembre (dualidad de peritos).
- STS 1167/2004, de 22 de octubre (protección de datos).
- STS 1194/2004, de 7 de diciembre (intervención telefónica).
- STS 1219/2004, de 10 de diciembre (protección de datos).
- STS 463/2005, de 13 de abril (intervención telefónica, identificación del titular).
- STS 501/2005, de 19 de abril (cadena de custodia).
- STS 1001/2005, de 19 de Julio (comunicante accidental).
- STS1029/2005, de 26 de septiembre (informe de inteligencia).
- STS 1302/2005, de 8 de noviembre (duplicidad de peritos).
- STS 1354/2005, de 16 de noviembre (grabación de la conversación por uno de los interlocutores).
- STS 1397/2005, de 30 de noviembre (acceso por la policía a la agenda de un móvil).
- STS 179/2006, de 14 de febrero (prueba pericial).
- STS 201/2006, de 1 de marzo (intervención de las comunicaciones, infracción de alcance constitucional y meras irregularidades procesales).

- STS 449/2006, de 17 de abril (conocimiento por los agentes policiales de los listados telefónicos de las agendas de teléfonos móviles)
- STS 515/2006, de 4 de abril (comunicante accidental).
- STS 556/2006, de 31 de mayo (inteligencia policial).
- STS 986/2006, de 19 de junio (protección de datos, art. 11.2 LOPD).
- STS 1281/2006, de 27 de diciembre (informes periciales no ratificados).
- STS 23/2007, de 23 de enero (intervención de teléfono distinto del investigado, a través de IMEI).
- STS 112/2007, de 16 febrero (acceso por la policía los números de contacto).
- STS 119/2007, de 16 de febrero (sobre informes de inteligencia).
- STS 203/2007, de 13 de marzo (falta la notificación al fiscal de la intervención telefónica)
- STS 209/2007, de 9 de marzo (captación de conversaciones por radiofrecuencia).
- STS 277/2007, de 13 de abril (derecho a la intimidad).
- STS 710/2007, de 27 de junio (informes de inteligencia policial).
- STS 768/2007, de 1 de octubre (hallazgo casual).
- STS 782/2007, de 3 de octubre (derecho a la intimidad, visionado por la policía de grabaciones efectuadas por un particular).
- STS 926/2007, de 13 de noviembre (intervención de comunicaciones, indicios).
- STS 236/2008, de 9 de mayo (acceso a direcciones IP, programa P2P).
- STS 249/2008, de 20 de mayo (captación del IMSI).
- STS 256/2008, de 14 de mayo (volcado de datos informáticos).
- STS 292/2008, de 28 de mayo (intercambio de archivos con el programa "Edonkey").
- STS 503/2008, 17 de julio (hallazgo casual).
- STS 739/2008, de 12 de noviembre (cesión de datos)
- STS 776/2008, de 18 de noviembre (captación de números IMSI).
- STS 785/2008, de 25 de noviembre (derecho a la intimidad, conversaciones en chats almacenados).
- STS 960/2008, de 26 de diciembre (intervención telefónica).
- STS 40/2009, de 28 de enero (transcripción de las grabaciones).
- STS 113/2009, de 12 de febrero (duplicidad de peritos).

- STS 221/2009, de 6 de marzo (cadena de custodia).
- Acuerdo del Pleno no jurisdiccional de la Sala II, de 26 de mayo de 2009.
- STS 480/2009, de 22 de mayo caso *Ekin-Kas-Xaki.* (volcado contenido de ordenador sin LAJ, informe de inteligencia policial, pericial informática).
- STS 509/2009, de 13 de mayo (irregularidad procesal que no vulnera el 18.3)
- STS 556/2009, de 16 de marzo (estafa mediante Phising).
- STS 691/2009, de 5 de junio (derecho fundamental a la intimidad).
- STS 704/2009, de 29 de junio (secreto en la intervención de comunicaciones).
- STS 707/2009, de 22 de junio (sobre los listados de llamadas telefónicas).
- STS 985/2009, de 13 octubre (informe de inteligencia policial).
- STS 1130/2009, de 10 de noviembre (desarrolla el Acuerdo del TS de 26 de mayo de 2009).
- STS 1190/2009, de 3 de diciembre (cadena de custodia).
- STS 1215/2009, de 30 de diciembre (sobre sistema SITEL).
- STS 1273/2009, de 17 de diciembre (sobre acceso por la policía al listado de llamadas entrantes y salientes de un teléfono móvil).
- STS 1315/2009, de 18 de diciembre (conocimiento por los agentes policiales de los listados telefónicos de las agendas de teléfonos móviles).
- STS 1319/2009, de 29 de diciembre (comunicante accidental).
- STS 1349/2009, de 29 de diciembre (cadena de custodia).
- STS 1362/2009, de 23 de diciembre (comunicante accidental).
- STS 84/2010, de 18 de febrero (intervención de teléfono de la hija del investigado).
- STS 90/2010, de 5 de febrero (ausencia de notificación al fiscal de la intervención).
- STS 93/2010, de 8 de febrero (cadena de custodia).
- STS 167/2010, de 24 de febrero (hallazgo casual).
- STS 239/2010, de 24 de marzo (grabación de conversaciones por uno de los interlocutores).
- STS 240/2010, de 24 de marzo (cadena de custodia).
- STS 247/2010, de 18 de marzo (recoge el Acuerdo del Pleno de la Sala 2ª 23-2-2010).
- STS 266/2010, de 31 de marzo (cadena de custodia).

- STS 309/2010, de 31 de marzo (Sobre obtención de número de teléfono).
- STS 372/2010, de 29 de abril (hallazgo casual).
- ATS 1051/2010, de 27 de mayo (cadena de custodia).
- STS 513/2010, de 2 de junio (sobre listados de llamadas telefónicas y aportación de las escuchas telefónicas a juicio).
- STS 605/2010, de 24 de junio (desarrolla el Acuerdo del TS de 26 de mayo de 2009).
- STS 680/2010, de 14 de julio (obtención de IP, autorización judicial para la cesión de datos).
- STS 744/2010, de 26 de julio (auto de intervención telefónica incoado en otra causa).
- STS 745/2010, de 26 de julio (intervención de teléfono a través de IMEI).
- STS 768/2010, 15 de septiembre (sobre nulidad de la prueba).
- STS 862/2010, de 4 de octubre (obtención de número de teléfono por la policía)
- STS 1110/2010, de 23 de diciembre (hallazgo casual en registro diferencia con el de la intervención telefónica).
- STS 1138/2010, de 16 de diciembre (intervención telefónica en otras diligencias).
- STS 2/2011, de 15 de febrero (conexión de antijuricidad).
- STS 53/2011, de 10 de febrero (cadena de custodia).
- STS 85/2011, de 7 de febrero (intervención telefónica, presunción de licitud en la obtención del número a intervenir, incorporación del material al juicio oral).
- STS 104/2011, de 1 de marzo (conocimiento por los agentes policiales de los listados telefónicos de las agendas de teléfonos móviles).
- STS 272/2011, de 12 de abril (desarrolla el Acuerdo del TS de 26 de mayo de 2009).
- STS 285/2011, de 20 de abril (introducción de las comunicaciones al juicio oral).
- STS 293/2011, de 14 de abril (destrucción de grabaciones).
- STS 320/2011, de 22 de abril (conexión de antijuricidad).
- STS 321/ 2011, de 26 de abril (conocimiento por los agentes policiales de los listados telefónicos de las agendas de teléfonos móviles).

- STS 493/2011, 26 de mayo (interceptación sin conocer la identidad del interlocutor).
- STS 539/2011, de 26 de mayo (hallazgo casual).
- STS 544/2011, de 7 de junio (firma electrónica).
- STS 565/2011, de 6 de junio (destrucción de registros, sistema SITEL).
- STS 629/2011, de 23 de junio (juicio de fiabilidad).
- STS 663/2011, de 7 de julio (conocimiento por los agentes policiales de los listados telefónicos de las agendas de teléfonos móviles).
- STS 789/2011, de 20 de julio (incorparción de las escuchas al juicio oral).
- STS 818/2011, de 21 de Julio (hallazgo casual intervención telefónica).
- STS 940/2011, de 27 de septiembre (intervención telefónica, motivación).
- STS 988/2011, de 30 de septiembre (conexión de antijuricidad).
- ATS de 5 de octubre de 2011 (rec.20137/2011) (competencia en un ataque de un hacker a páginas web).
- STS 1044/2011, de 11 de octubre (secreto en la intervención de comunicaciones).
- STS 1045/2011, de 14 de octubre (registro de ordenadores).
- STS1078/2011, de 24 de octubre (presunción de licitud en la obtención del número de teléfono a intervenir por parte de la policía)
- STS 1115/2011, de 17 de noviembre (captación de IMSI e IMEI).
- STS 1161/2011, de 31 de octubre (cartas nigerianas, envío masivo de correos).
- STS 1299/2011, de 17 de noviembre (obtención IP, programa P2P).
- STS 112/2012, de 23 de febrero (aportación a juicio de las escuchas telefónicas).
- STS 207/2012, de 12 de marzo (presunción de licitud en la obtención del número de teléfono).
- STS 315/2012, de 22 de marzo (aportación de escuchas telefónicas mediante documental).
- STS 380/2012, de 16 de mayo (destrucción de grabaciones).
- STS 410/2012, de 17 de mayo (destrucción de grabaciones).
- STS 433/2012, de 1 de junio (bilateralidad en la intervención).
- STS 503/2012, de19 de junio (desarrolla el Acuerdo del TS de 26 de mayo de 2009).

- STS 554/2012, de 4 de julio (firma electrónica).
- STS 616/2012, de 10 de julio (hallazgo casual intervención telefónica).
- STS 635/2012, 17 de julio (intervención telefónica, motivación).
- STS 636/2012, de 13 de Julio (hallazgo casual).
- STS 658/2012, de 13 de julio (intervención telefónica, indicios).
- STS 654/2012, de 20 de julio (conexión de antijuiricidad, confesión).
- STS 722/2012, de 2 de octubre (firma electrónica).
- STS 740/2012, de 10 de octubre (intervención telefónica, elementos indiciarios, hallazgo casual).
- STS 712/2012, de 26 de septiembre (comunicante accidental).
- STS 751/2012, de 28 de septiembre (autorización judicial que se deriva de otra intervención de comunicaciones).
- STS 794/2012, de 11 de octubre (destrucción de grabaciones).
- STS 811/2012, de 30 de octubre (conexión de antijuricidad).
- STS 821/2012, de 31 de octubre (conexión de antijuricidad).
- STS 862/2012, de 31 de octubre (hallazgo casual de información suministrada por policía extranjera).
- STS 884/2012, de 12 de noviembre (*notitia criminis"* procedente de autoridades extranjeras, SMS).
- STS 48/2013, 23 de enero (hallazgo casual).
- STS 143/2013, de 28 de febrero (destrucción de grabaciones, firma electrónica).
- STS 165/2013, de 26 de marzo (transcripción de las conversaciones).
- STS 298/2013, de 13 de marzo (grabación subrepticia de una conversación con autorización de uno de los interlocutores).
- STS 301/2013, de 18 de abril (conexión de antijuricidad).
- STS 342/2013, del 17 de abril (derecho al propio entorno virtual, diligencia de volcado).
- STS 419/2013, de 14 de mayo (hallazgo casual en captación de conversaciones).
- STS 427/2013, 10 de mayo (provocación delictiva).
- STS 695/2013, de 22 de julio (captación de conversaciones radiotelegráficas).

- STS 715/2013, de 27 de septiembre (incorporación del material al juicio oral).
- STS 912/2013, de 4 de diciembre (conexión de antijuricidad).
- STS 17/2014, de 28 de enero (hallazgo casual en registro).
- STS 113/2014, de 17 de febrero (conexión de antijuricidad).
- ATS 19 de febrero de 2014 (cuestión de competencia 20768/2013 sobre phising).
- STS 157/2014, de 5 de marzo (hallazgo casual policía extranjera).
- STS 246/2014, de 2 de abril (obtención de IMEI e IMSI).
- STS 251/2014, de 13 de abril (intervención telefónica procedente de autoridad policial extranjera).
- STS 444/2014, de 9 de junio (intimidad, agenda de móvil versus listado de llamadas).
- STS 558/2014 de 8 de julio (hallazgo casual diferencias entre registro e intervención de telecomunicaciones).
- STS 587/2014, de 18 de julio (cadena de custodia).
- ATS 1647/2014, de 16 de octubre (custodia del material informático).
- STS 795/2014, de 20 de noviembre ("*notitia criminis"* procedente de autoridades extranjeras).
- STS 850/2014, de 26 de noviembre (comunicaciones telemáticas).
- STS 867/2014, de 11 de diciembre (incorporación de las escuchas al juicio oral).
- STS 877/2014, de 22 de diciembre (intervención de ADSL).
- STS 96/2015 de 5 de febrero (hallazgo casual escuchas telefónicas).
- STS 97/2015, de 24 de febrero (derecho al entorno virtual).
- STS 106/2015 de 19 de febrero (enaltecimiento del terrorismo a través de youtube).
- STS 138/2015, de 13 de marzo (firma electrónica).
- STS 153/2015, de 18 de marzo (indicios en la intervención de comunicaciones).
- STS 203/2015, de 23 de marzo (sobre confidencias que motivan un auto de intervención telefónica).
- STS 300/2015, de 19 mayo (prueba de una conversación en redes sociales).
- STS 309/2015, de 22 de mayo (sobre intervención de las comunicaciones).

- STS 511/2015, de 21 de julio (conexión de antijuricidad).
- ATS de 29 de octubre de 2015 (sección 1ª) resuleve cuestión de competencia negativa en la modalidad de ciberdelito consistente en extorsionar a personas que previamente habían sido grabadas practicando cibersexo.
- STS 745/2015, de 23 de noviembre (motivación por remisión).
- STS 747/2015, de 19 de noviembre (nulidad de la diligencia de instalar dispositivos electrónicos acoge la STC 145/2014, de 22 de septiembre).
- STS (Sala V) 25 de noviembre de 2015 (pericial informática).
- STS 754/2015, de 27 de noviembre (mensajería instantánea).
- STS 786/2015, de 4 de diciembre (derecho fundamental a la intimidad recoge la STC 173/2011, de 7 de noviembre).
- STS 864/2015, de 10 de diciembre (derecho a la intimidad, ciberacoso, intervención de la policía en caso de urgencia).
- STS 834/2015, de 23 de diciembre (hallazgo casual).
- STS 204/2016, de 10 de marzo (derecho a la intimidad, intervención policial en caso de urgencia, derecho al entorno virtual).
- ATS 16 de marzo de 2016 (cuestión de competencia 20040/2016). (sobre competencia de introducción de material pornográfico en la web).
- STS 277/2016, de 6 de abril (agente encubierto, cadena de custodia).
- STS 300/2016, de 11 de abril (conexión de antijuricidad).
- STS 551/2016, de 22 de junio (Obtención de IMSI, IMEI y PIN blackberry).
- STS 623/2016 de 13 julio (comisión del delito de enaltecimiento del terrorismo a través de twiter).
- STS 650/2016, de 15 de julio (conexión de antijuricidad, confesión).
- STS 704/2016, de 14 de septiembre (intervención telefónica, indicios).
- STS 714/2016, de 26 de septiembre (cadena de custodia).
- STS 820/2016, de 2 de noviembre (sobre delito de odio a través de Facebook).
- STS 4/2017, de 18 de enero (discurso de odio en twiter)

IV. AUDIENCIA NACIONAL.

- SAN 2/2012, de 17 de enero (enaltecimiento del terrorismo en la red social Tuenti)
- SAN 8/2014, de 31 de marzo (enaltecimiento del terrorismo a través de youtube).
- SAN 23/2015, de 30 de septiembre (ciberterrorismo, facebook).
- SAN 13/2016, de 1 de junio (agente encubierto y provocación delictiva).
- SAN 20/2016, de 18 de julio (discurso del odio en twiter).

V. AUDIENCIAS PROVINCIALES.

- SAP Valencia (sección 3ª) 322/2002, de 8 julio (pericial sobre el destino de correos electrónicos).
- SAP Valladolid (sección 2ª) 549/2002, de 22 de julio (aportación de correos electrónicos).
- SAP Cáceres (sección 2ª) 127/2002 de 30 diciembre 2002 (correo electrónico con remitente desconocido).
- SAP Valencia 2/2003, de 11 de enero (sobre peritos-Inspectores de finanzas en un delito fiscal).
- AAP Barcelona (sección 15) 46/2006, de 2 de febrero (pericial informática sobre borrado de datos).
- SAP Barcelona, (Sección 7ª) 95/2008 de 29 de enero (sobre peritos expertos en informática).
- Auto de la Audiencia Provincial de Vizcaya (Sección 2ª) 175/2008, de 31 de marzo (sobre pericias particulares).
- SAP Burgos 13/2009, de 9 de marzo (sobre prueba pericial).
- Auto de la AP Castellón (sección 1ª) 367/2010 de 14 de octubre (pericial informática).
- SAP Madrid (sección 1ª) 531/2010 de 21 de diciembre (pericial informática).
- SAP de Madrid (sección 29) 96/2011, de 8 de noviembre (dualidad de peritos).

- SAP Las Palmas (sección 2ª) 180/2011, de 15 de julio (incorporación del material informático mediante testitfical).
- SAP de Murcia (sección 3ª) 85/2011 de 25 de octubre (cadena de custodia de un disco duro).
- SAP de Málaga (sección 7ª) 19/2013 de 21 de marzo, (cadena de custodia de un Iphone).
- SAP de Valencia (sección 2ª) 254/2013 de 25 marzo (conexión de antijuricidad)
- SAP de Alicante (sección 8ª) 4/2014, de 9 de enero (prueba de WhatsApp en ámbito civil).
- SAP de Huelva (sección 3ª) 48/2014, de 20 de febrero (conexión de antijuriciad).
- SAP Córdoba (Sección 3ª) 363/2014, de 18 julio (sobre rastreo policial de archivos informáticos).
- SAP de Madrid (sección 26) 533/2014, de 24 de julio (estados de WhatsApp).
- SAP de Valladolid (sección 4ª) 119/2015, de 13 de abril (sobre estados de WhatsApp).
- SAP Madrid 840/2015, 23 de octubre (no se precisa autorización judicial para conseguir lo que es público).
- Auto 940/2015 de la Audiencia Provincial de Málaga (Sección 9ª), de 18 de noviembre de 2015, de planteamiento de cuestión de inconstitucionalidad de la Ley de Equipos Conjuntos de Investigación.
- Auto (Sección 4ª) de la Audiencia de Tarragona de 6 de abril de 2016 (Rollo de apelación penal 628/2015). De planteamiento de cuestión prejudicial sobre si la reforma de la LECrim relativa a la cesión de datos es compatible con las exigencias contenidas en la STJUE de 8 de abril de 2014.

VI. OTROS TRIBUNALES.

- STJUE, Gran Sala, de 8 de abril de 2014 (casos C-293/2012 y C- 594/2012). declaración de invalidez de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006.

BIBLIOGRAFÍA

- ABEL LLUCH, XAVIER y RICHARD GONZÁLEZ (Dir). "Estudios sobre Prueba Penal. Volumen III. Actos de investigación y medios de prueba en el proceso penal: diligencias de instrucción, entrada y registro, intervención de comunicaciones, valoración y revisión de la prueba en vía de recurso". Ed. La Ley, Madrid, 2013.

- ABEL LLUCH, XAVIER. *Nuevas tecnologías e investigación penal* en "Estudios sobre Prueba Penal. Volumen III. Actos de investigación y medios de prueba en el proceso penal: diligencias de instrucción, entrada y registro, intervención de comunicaciones, valoración y revisión de la prueba en vía de recurso" (Abel Lluch y Richard González, Dir). Ed. La Ley, Madrid, 2013.

- ADÁN DEL RÍO, CARMEN. "La persecución y sanción de los delitos informáticos". EGUZKILORE nº 20. San Sebastián, Diciembre 2006.

- AGUILAR CÁRCELES, MARTA MARÍA. "Cibercrimen y cibervictimización en Europa: instituciones involucradas en la prevención del ciberdelito en el Reino Unido". Revista Criminalidad, vol. 57 nº 1, 20015.

- AGUILERA MORALES, MARIEN. "El exhorto europeo de investigación: a la búsqueda de la eficacia y la protección de los derechos fundamentales en las investigaciones penales transfronterizas". Boletín del Ministerio de Justicia nº 2145 Agosto 2012 www.mjusticia.es/bmj

- AGUSTINA SANLLEHÍ, JOSÉ R. "Interrogantes en torno a las diligencias preliminares ante la ciberdelincuencia. Sobre la garantía del derecho a la intimidad en el registro del ordenador (a propósito de la STC 173/2011)". La ley penal, jurisprudencia nº 98-99, Noviembre-diciembre 2012.

- AGUSTINOY GUILAYN, ALBERT Y MONCLÚS RUIZ, JORGE. "Aspectos legales de las redes sociales". Colección Práctica Jurídica. Ed. Bosch, Barcelona, 2016.

- ALONSO GARCÍA, JAVIER. "Derecho penal y redes sociales". Ed. Aranzadi Thomson Reuters, Navarra, 2015.

- ALONSO-CUEVILLAS SAYROL, JAIME (Dir). "El nuevo proceso penal tras la reforma de 2015". Ed. Atelier, Barcelona, 2016.

- ANARTE BORRALLO, ENRIQUE y DOVAL PAIS, ANTONIO. "Efectos de la reforma de 2015 en los delitos contra la intimidad". Diario La Ley nº 8744, Ed. La Ley, 19 de Abril de 2016.

- ALVAREZ CIENFUEGOS-SUAREZ, JUAN MANUEL."Los delitos de falsedad y los documentos generados electrónicamente. Concepto procesal y material de documento: nuevas técnicas", Cuadernos de Derecho Judicial, La nueva delincuencia II. C.G.P.J., Madrid, 1993.

- ALVAREZ MONTOYA, WILLIAM. 6.1. INTRODUCCIÓN. Breve Historia de Internet. En http://www.unalmed.edu.co/~incominf/W8070[6-1].htm. 8/10/2014 a las 16.27.

- ALVAREZ OREJA-EGAÑA, RAFAEL. "El ciberdelito: la contribución de las estrategias de seguridad a la lucha contra la ciberdelincuencia: armas jurídicas contra el nuevo enemigo". Cuadernos de la Guardia Civil: Revista de seguridad pública, nº 46, 2012.

- ANGUAS BALSERA, JOAQUÍM, La cadena de valor en la prueba con base informática. http://www.anguas.com/e1m6/Docs/Foro_Legal_La%20cadena_de_valor_de_la_prueba_informatica.pdf.

- ANGUIANO JIMÉNEZ, JOSÉ MARÍA. "El valor probatorio de las comunicaciones electrónicas". XI Congreso Nacional de la Abogacía. http://www.abogacia.es/2016/04/17/el-valor-probatorio-de lascomunicacioneselectronicas-jose-maria-anguiano-xi-congreso-nacional-de-la-abogacia/

- ARANGÜENA FANEGO, CORAL. "Emisión y ejecución en España de órdenes europeas de protección (Ley de reconocimiento mutuo de resoluciones penales en la Unión Europea y transposición de la Directiva 2011/99/UE)" Revista de Derecho Comunitario Europeo nº 51, Mayo/Agosto 2015.

- ARQUÉS SOLDEVILA, JOSEP MARIA. "Pericial informática en un caso tipo de pornografía infantil". Revista de derecho y proceso penal nº 30, Aranzadi. Ene-Abr 2013.

- AROCA MONTOLÍO, CONCEPCIÓN y MIRÓ PÉREZ, CAMILO. "Los ciberdelitos y sus consecuencias en las cibervíctimas". Pedagogía multidisciplinar para la salud: claves para la intervención psico-educativa, socio-comunitaria y físico-ambiental. Ed. Tirant lo Blanch, Valencia, 2014.

- ASENCIO MELLADO, JOSÉ MARÍA. "Prueba ilícita: declaración y efectos", en Revista General de Derecho nº 26, año 2012.

- ASENCIO MELLADO, JOSÉ MARÍA. "Intervención de las comunicaciones y la prueba ilícita". Universidad de Alicante. Mayo de 2011. https://www.unifr.ch/ddp1/derechopenal/articulos/a_20110507_02.pdf

- BACARIA MARTRUS, JORDI. "Las novedades del Reglamento General Europeo de Protección de Datos". Revista Economist & Jurist nº 201. Ed. Difusión Jurídica y Temas de Actualidad. Madrid 2016.

- BACHMAIER WINTER, LORENA. "La propuesta de Directiva Europea sobre la orden de investigación penal: valoración crítica de los motivos de denegación". Diario La Ley nº 7992, 28 de diciembre de 2012.

- BAÑON AGUILERA, JUAN MARÍA."Las medidas de investigación tecnológica". http://decrim.weebly.com/derecho/-lasmedidas-de-investigacion-tecnologicas-iv-el-registro-de-dispositivos-de almacenamientomasivo-y-el-registro-remoto-sobre-equipos-informaticos.

- BARRIO ANDRÉS, MOISÉS. "Los delitos cometidos en internet: marco comparado, internacional y derecho español tras la reforma penal de 2010". La Ley Penal: revista de derecho penal, procesal y penitenciario nº 86. Madrid, 2011.

- BARROSO TOLEDO, REINA. "Los Delitos en Internet: Un enfoque desde la pornografía infantil en la red". F@ro: Revista teórica del Departamento de Ciencias de la Comunicación nº 13, 2011.

- BARRY M. LEINER, VINTON G. CERF, DAVID D. CLARK, ROBERT E. KAHN, LEONARD KLEINROCK, DANIEL C. LYNCH, JON POSTEL, LAWRENCE G. ROBERTS, STEPHEN WOLFF Ilustraciones de KEVIN GRIFFIN Traducción: ALONSO ALVAREZ, LLORENÇ PAGÉS "Una breve historia de Internet (Primera Parte)", http://www.ati.es/DOCS/internet/histint/histint1.html 02/10/2013 0:35.o http://www.internetsociety.org/internet/what-internet/history-internet/brief-history internet 01/10/2014 14.15.

- BARRY M. LEINER, VINTON G. CERF, DAVID D. CLARK, ROBERT E. KAHN, LEONARD KLEINROCK, DANIEL C. LYNCH, JON POSTEL, LAWRENCE G. ROBERTS, STEPHEN WOLFF Ilustraciones de KEVIN GRIFFIN Traducción: ALONSO ALVAREZ, LLORENÇ PAGÉS "Una breve historia de Internet (Segunda Parte)", http://www.ati.es/DOCS/internet/histint/histint2.html 02/10/2013 0:36.

- BAYO DELGADO, JOAQUÍN, CASERO LINARES, LUIS, DEL CERRO ESTEBAN, JOSE ANTONIO, DREWER, DANIEL, FRÍAS MARTÍNEZ, EMILIO, MARCOS AYJÓN, MIGUEL, MICHAEL ALEXANDER, PETER, MORÁN MARTÍNEZ, ROSANA, RODRÍGUEZ VALLS, Mª TERESA, SUTTON, GRAHAM y GUTIÉRREZ ZARZA, ÁNGELES (coord.). "Nuevas tecnologías, protección de datos y proceso penal" Ed. La Ley grupo Wolters Kluwer, Madrid 2012.

- BERMÚDEZ GONZÁLEZ, JORGE. Deber de colaboración de particulares en LECrim. Ponencia presentada en el curso de Formación de Fiscales "Uso de las nuevas tecnologías y nuevas formas de delincuencia" que se celebró en el Centro de Estudios Jurídicos los días 27 al 28 de octubre de 2016. http://www.cej-mjusticia.es.

- BUENO DE MATA, FEDERICO. "Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica". Diario La Ley nº 8627, Ed. La Ley, 19 de Octubre de 2015.

- BUENO DE MATA, FEDERICO. *Un centinela virtual para investigar delitos cometidos a través de las redes sociales. ¿ Deberían ampliarse las actuales funciones del agente encubierto en Internet?* En "El proceso penal en la sociedad de la información. Nuevas tecnologías para investigar y probar el delito" (PÉREZ GIL Coord). Ed. La Ley, Madrid, 2012.

- BUJOSA VADELL, LORENZO M y MARTÍN GARCÍA, ANTONIO LUIS. "La obtención de prueba en materia penal en la Unión Europea". Ed. Atelier, Barcelona, 2016.

- BUJOSA VADELL, LORENZO M. "Ley Orgánica 6/2014, de 29 de octubre, complementaria de la Ley de reconocimiento mutuo de resoluciones penales en la Unión Europea, por la que se modifica la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial [BOE n.º 263, de 30-X-2014] y Ley 23/2014. AIS: Ars Iuris Salmanticensis

[Internet]. 1 Junio 2015. http://campus.usal.es/~revistas_trabajo/index.php/ais/article/view/13939

- CABEZUDO BAJO, MARIA JOSÉ. *Fiabilidad y Licitud de la prueba de ADN en la UE y en España,* en "El proceso penal en la Sociedad de la Información, nuevas tecnologías para investigar y probar el delito"(Pérez Gil, Coord.). Ed. La Ley, Madrid 2012.

- CABEZUDO RODRÍGUEZ, NICOLÁS. "Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal". Boletín del Ministerio de Justicia nº 2186. La reforma del proceso penal. Febrero de 2016.

- CABEZUDO RODRÍGUEZ, NICOLÁS. "Omisiones y recelos del legislador procesal ante los medios de prueba tecnológicos". Diario La Ley nº 6158. Ed. La Ley, 2004.

- CANO PAÑOS, MIGUEL ÁNGEL. "El Caso "Khaled Kelkal". Una clave para entender la radicalización islamista en la europa del año 2015", Revista Electrónica de Ciencia Penal y Criminología nº17-09, 20016.

- CARRETERO SÁNCHEZ, SANTIAGO. "Las redes sociales y su impacto en el ataque a los derechos fundamentales: aproximación general". Diario La Ley nº 8718, 9 de Marzo de 2016.

- CASANOVA MARTÍ, ROSER. "La captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos." Diario La Ley nº 8674, 4 enero 2016.

- CASTILLEJO MANZANARES, RAQUEL. "Hacia un nuevo proceso penal. Cambios necesarios". Ed. La Ley, Madrid, octubre 2010.

- CASTILLEJO MANZANARES, RAQUEL. "La prueba en el proceso penal. el documento electrónico". Revista de Derecho Penal nº 29, 2010.

- CAYÓN PEÑA, JUAN y GARCÍA SEGURA, LUIS A. "Hacia un nuevo enfoque del conflicto ciber en el ámbito empresarial". Diario La Ley nº 8577, 2015.

- CHICHARRO LÁZARO, ALICIA. "La labor legislativa del Consejo de Europa frente a la utilización de Internet con fines terroristas". IDP: revista de Internet, derecho y política, revista d'Internet, dret i política nº 9, 2009.

- CHOCLÁN MONTALVO, JOSÉ ANTONIO. *Infracciones patrimoniales en los procesos de transferencia de datos*. En "El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales" (ROMEO CASABONA Coord). Ed. Comares, Granada, 2006.

- CLIMENT BARBERÁ. JUAN. "La justicia Penal en Internet. Territorialidad y competencias penales". Cuadernos de derecho judicial, internet y derecho penal nº 10. CGPJ Madrid, 2001.

- COLOMER HERNÁNDEZ, IGNACIO. "La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea" (dir. Oubiña Barbolla, S). Ed. Aranzadi, Pamplona, 2015.

- CONDE-PUMPIDO TOURÓN, CÁNDIDO. "La reforma procesal. Registro de sistemas informáticos, ampliación del registro a otros sistemas. El registro remoto de dispositivos informáticos (arts 588 sexies y 588 septies LECrim)". Ponencia presentada en las Jornadas de especialistas de criminalidad informática. 2016. www.cej-mjusticia.es.

- CONTRERAS CEREZO, PABLO. "Comentario a la STC 173/2011". Diario La Ley nº 7819, Sección La Sentencia del día del TC, marzo, 2012.

- CURRAN JAMES. *Reinterpreting Internet history*. En "Handbook of Internet Crime". Ed. Willan Publishing, Devon, UK y simultáneamente Portland, Oregón. USA. 2010.

- DE LA MATA BARRANCO, NORBERTO J Y HERNÁNDEZ DÍAZ, LEYRE, "El delito de daños informáticos: una tipificación defectuosa". Estudios Penales y Criminológicos, vol. XXIX, 2009.

- DELGADO MARTIN, JOAQUÍN. "Investigación tecnológica y prueba digital en todas las jurisdicciones". Ed. La Ley, Madrid, noviembre 2016.

- DELGADO MARTIN, JOAQUÍN. "Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015". Diario La Ley nº 8693, Sección Doctrina, 2 de Febrero de 2016.

- DELGADO MARTÍN, JOAQUÍN. "La prueba del whatsapp", Diario La Ley nº 8605, 2015.

- DELGADO MARTÍN, JOAQUÍN. "Responsabilidad penal de los proveedores de servicios en la sociedad de la información: especial referencia a las páginas web de enlaces", Diario La Ley nº 8254, 2014.

- DELGADO MARTIN, JOAQUÍN. "Derechos fundamentales afectados en el acceso al contenido de dispositivos electrónicos para la investigación de delitos". Diario La Ley nº 8202, Sección Doctrina, 29 Noviembre 2013.

- DELGADO MARTIN, JOAQUÍN, "La prueba electrónica en el proceso penal". Diario La Ley nº 8167, Sección Doctrina, 10 Octubre 2013.

- DE JORGE MESAS, LUIS FRANCISCO. *La incorporación de las nuevas tecnologías informáticas y de telecomunicaciones al proceso penal* en "Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia" (Velasco Núñez, E Coord). Cuadernos de derecho judicial, Consejo General del Poder Judicial, Madrid 2007.

- DE URBANO CASTRILLO, EDUARDO. "Los delitos informáticos tras la reforma del CP de 2010". Revista Aranzadi Doctrinal nº 9/2011 parte Estudio. Pamplona, 2011.

- DE URBANO CASTRILLO, EDUARDO. *El documento electrónico: aspectos procesales*, en "Internet y Derecho Penal" (López Ortega, Dir). Escuela Judicial CGPJ, 2001.

- DÍAZ DÍAZ, PATRICIA. "Medios de prueba y nuevas tecnologías". Máster Universitario en abogacía. Universidad de Oviedo. Mayo 2014. http://digibuo.uniovi.es/dspace/bitstream/10651/29656/5/TFM_Diaz%20Diaz,Patricia.pdf

- DÍAZ GÓMEZ, ANDRÉS, "El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest". Revista electrónica del Departamento de Derecho de la Universidad de La Rioja, REDUR 8, diciembre 2010.

- DOLZ LAGO, MANUEL JESÚS. "Oído a los delitos de odio (Algunas cuestiones claves sobre de la reforma del art. 510 CP por LO 1/2015)". Diario La Ley, nº 8712, 1 de marzo de 2016.

- ÉCIJA BERNAL, ÁLVARO. "Ciberespacio, darkweb y ciberpolicía". Diario La Ley nº 2, Sección Ciberderecho, 4 de Enero de 2017.

- ÉCIJA BERNAL, ÁLVARO. “El Ciberespacio: una herramienta de poder”. Actualidad Jurídica Aranzadi nº 879, año 2014.

- ENCINAR DEL POZO, MIGUEL ÁNGEL. “La invalidez de la Directiva sobre Conservación y Cesión de los Datos relativos a las Comunicaciones”. Revista SEPIN SP/DOCT/18682, 07 de noviembre de 2014.

- ENGDAHL SYLVIA (Coord). “Cybercime. Issues on Trial”. Ed. Gale Cengage Learning. USA, 2010.

- ETXEBERRÍA GURIDI, FRANCISCO. *Videovigilancia y su eficacia en el proceso penal,* en “El proceso penal en la sociedad de la información. Nuevas tecnologías para investigar y probar el delito”(PÉREZ GIL Coord). Ed. La Ley, Madrid, 2012.

- FERNANDEZ GALLARDO, JAVIER ÁNGEL. “La cámara oculta en el proceso penal.” Revista Penal nº 38, 2016.

- FERREYROS SOTO, CARLOS. *Aspectos metodológicos del delito informático*, en “Informática y derecho”. Revista iberoamericana de derecho informático nº 9-11, 1996.

- FIGUEROA NAVARRO, CARMEN Y DEL AMO RODRÍGUEZ, ANTONIO. “La cadena de custodia de las pruebas y los protocolos de actuación de la policía científica”. Policía Científica. 100 años de ciencia al servicio de la Justicia. Ministerio del Interior. Material de las Jornadas Centenario de la Policía Científica Española, junio 2011.

- FLORES PRADA, IGNACIO. “Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia”. Revista Electrónica de Ciencia Penal y Criminología nº 17-21, 2015.

- FRAGO AMADA, JUAN ANTONIO. "La prueba en los delitos cometidos a través de redes sociales. www.legaltoday.com, práctica jurídica. 23 de mayo de 2012.

- FRÍAS MARTÍNEZ, EMILIO. "ADN y privacidad en el proceso penal". Diario La Ley nº 8160, 2013.

- FRÍAS MARTÍNEZ, EMILIO. "Obtención, tratamiento y uso de datos personales por el Ministerio Fiscal". La Ley penal nº 71, Mayo de 2013.

- FRÍAS MARTÍNEZ, EMILIO. "El acceso a los datos de carácter personal por la Policía. Referencia a los datos de la Seguridad Social". Noticias Jurídicas, Julio 2012, y http://articulosdeinterespolicial.blogspot.

- FRÍAS MARTÍNEZ, EMILIO. "Bases de datos policiales. Cancelación de sus datos. Valoración probatoria". Diario La Ley nº 7928, 21 de Septiembre de 2012.

- FRÍAS MARTÍNEZ, EMILIO. "Los sistemas de videovigilancia: la protección de datos y sus efectos en el proceso penal". Diario La Ley nº 7396, 2010.

- FRÍAS MARTÍNEZ, EMILIO. "Protección y tratamiento de datos personales por el Ministerio Fiscal". La ley penal: revista de derecho penal, procesal y penitenciario nº 71, 2010.

- FURNELL STEVEN. *Hackers, viruses and malicious software,* en "Handbook of Internet Crime". Ed. Willan publishing. Cullompton, Devon (UK) 2010.

- FURNELL STEVEN. "Cybercrime. Vandalizing the information society". Ed. Addison-Wesley, A Pearson Education Limited, Great Britain 2002.

- GERKE MARCO. “Comprensión del ciberdelito: fenómenos, dificultades y respuesta jurídica”. Sector de Desarrollo de las Telecomunicaciones de la UIT. Ginebra (Suiza) Septiembre de 2012. en: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

- GIMÉNEZ-SALINAS FRAMIS, ANDREA. *La delincuencia organizada en europa: extensión, factores facilitadores y rasgos principales* en “La Lucha contra el crimen organizado en la Unión Europea”. Documentos de Seguridad y Defensa 48. Centro Superior de Estudios de la Defensa Nacional. Ed. Ministerio de Defensa, Madrid 2012.
http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/docSegyDef/fich eros/048_LA__LUCHA_CONTRA_EL_CRIMEN_ORGANIZADO_EN_LA_UNION EUROPEA.pdf.

- GIMENO SENDRA, VICENTE. “Derecho Procesal Penal”. Ed. Thomson Reuters, Navarra, octubre 2015.

- GIMENO BEVIÁ, JORDI. “Análisis crítico de la reforma de la LECrim 2015”. Revista Aranzadi de Derecho y Proceso Penal nº 40 (Octubre-Diciembre)Legislación, 2015.

- GÓMEZ ORBANEJA, EMILIO Y HERCE QUEMADA, VICENTE. “El Derecho Procesal Penal”. Ed. Por los autores, Madrid, 1972.

- GONZÁLEZ-CUELLAR SERRANO, NICOLÁS. “Proporcionalidad y derechos fundamentales en el proceso penal”, Ed. Colex, Madrid, 1990.

- GONZÁLEZ HURTADO, JORGE ALEXANDRE. “Delincuencia informática: daños informáticos del artículo 264 del código penal y propuesta de reforma”. Tesis doctoral, Universidad Complutense de Madrid, departamento de derecho penal, Madrid, 2013.

- GONZÁLEZ MONJE, ALICIA. "La presunción de inocencia en la Unión Europea: Directiva 2016/343 del Parlamento Europeo y del Consejo de 9 de marzo de 2016 por la que se refuerzan en el proceso penal determinados aspectos de la presunción de inocencia y el derecho a estar presente en el juicio." Revista General de Derecho Europeo nº 39, 2016.

- GONZÁLEZ-MONTES SÁNCHEZ, JOSÉ LUIS. "Reflexiones sobre el Proyecto de Ley Orgánica de modificación de la LECrim para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas". Revista electrónica de ciencia penal y criminología nº 17-06, junio 2015.

- GONZÁLEZ LÓPEZ, JUAN JOSÉ. *Intervención de comunicaciones: nuevos desafíos, nuevos límites* en "El proceso penal en la Sociedad de la Información. Las nuevas tecnologías para investigar y probar el delito"(PÉREZ GIL Coord). Ed. La Ley. Madrid, 2012.

- GONZÁLEZ LÓPEZ, JUAN JOSÉ. "Comentarios a la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones". Revista General de Derecho Procesal nº 16, 2008.

- GONZÁLEZ LÓPEZ, JUAN JOSÉ, "Los datos de tráfico de las comunicaciones electrónicas en el proceso penal", Ed. La Ley, Madrid 2007.

- GONZÁLEZ LÓPEZ, JUAN JOSÉ. *Retención de datos de tráfico de las telecomunicaciones y proceso penal*, en VVAA, "Estudios jurídicos sobre la Sociedad de la Información y nuevas tecnologías". Libro con motivo del XX Aniversario de la Facultad de Derecho, Servicio de Publicaciones de la Universidad de Burgos. Burgos 2005.

- GONZÁLEZ PÉREZ, JUAN JOSÉ. *Utilización en el proceso penal de datos vinculados a las comunicaciones electrónicas recopilados sin indicios de comisión*

delictiva, en "Protección de datos y proceso penal", Ed. La Ley, 2010

- GONZÁLEZ RUS, JUAN JOSÉ, *Precisiones conceptuales y político-criminales sobre la intervención penal en Internet*, en "Delito e informática: algunos aspectos," Cuadrernos Penales José Mª Lidón nº 4, Universidad de Deusto, Bilbao, 2007.

- GONZÁLEZ RUS JUAN JOSÉ. *Los ilícitos en la red (I): hackers, crakers cyberpunks, sniffers, denegación de servicios y otros comportamientos semejantes*. En "El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales" (Romeo Casabona, Coord.) Ed. Comares, Granada, 2006.

- GUDÍN RODRÍGUEZ-MAGARIÑOS, FAUSTINO. **"**Sobre el eventual futuro predominio del tipo telemático del art. 399 bis.3 CP tras la desaparición de la estafa telemática cometida a través del uso de una tarjeta de crédito". Artículo Monográfico. Ed. Sepín/DOCT/18927, marzo 2015.

- GUDÍN RODRÍGUEZ-MAGARIÑOS, FAUSTINO. "Incorporación al proceso del material informático intervenido durante la investigación penal". Boletín del Ministerio de Justicia nº 2163, febrero de 2014.

- GUERRERO PALOMARES SALVADOR. "La denominada prueba de inteligencia policial o pericial de inteligencia". Revista Aranzadi de derecho y proceso penal nº 25, 2001.

- GUTIÉRREZ FRANCÉS, MARILUZ. *Problemas de aplicación de la Ley Penal en el espacio virtual.* En "El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales" (Romeo Casbona, Coord). Ed. Comares, Granada, 2006.

- GUTIÉRREZ ROMERO, FRANCISCO MANUEL. "Algunas claves de la reforma de la Ley de Enjuiciamiento Criminal". Revista Aranzadi Doctrinal nº 2/2016 parte Comentario, 2 de mayo de 2016.

- HERNÁNDEZ DÍAZ, LEYRE. "El Delito Informático", Cuaderno del Instituto Vasco de Criminología nº 23, 2009.

- HERNÁNDEZ GARCÍA, LUIS FERNANDO. "Ciberseguridad; Respuesta global a las amenazas cibernéticas del S.XXI, las ciberamenazas, un nuevo reto para la jefatura de información de la Guardia Civil". Cuadernos de la Guardia Civil: Revista de seguridad pública nº 49, 2014.

- HERNÁNDEZ GUERRERO, F.J. y ALVAREZ DE LOS RIOS, J.L.: "Medios informáticos y proceso penal", en Estudios Jurídicos, Ministerio Fiscal IV, CEJAJ, Madrid, 1999.

- HERNÁNDEZ RAMOS, MARIO. "Una vuelta de tuerca más a las relaciones en materia de protección de datos entre la UE y los Estados Unidos. La invalidez de la Decisión Puerto Seguro." Revista General de Derecho Europeo nº 39, Mayo 2016.

- HERRERO-TEJEDOR ALGAR, FERNANDO. Capítulo VIII. *Delitos Informáticos*. Cuaderno de derecho para ingenieros. Cuaderno Duodédimo: La Nueva Reforma del Código Penal volumen 12, año 2012.

- HERRERO-TEJEDOR ALGAR, FERNANDO. *La libertad de expresión en internet*. En "Estudios jurídicos, Ministerio Fiscal. Criminalidad Informática e Internet". Ministerio de Justicia, Madrid IV, 1999.

- HUERTA CEREZUELA, VÍCTOR. "Un nuevo sistema para combatir el cibercrimen mitigando las vulnerabilidades". RUIDERAe: Revista de Unidades de Información, Descripción de Experiencias y Resultados Aplicados nº 7, 2015.

- INCE DARREL. "The Computer. A very short introduction". Ed. Oxford University Press. New York (EE.UU) 2011.

- INDA ORTIZ DE ZÁRATE. F. JAVIER. “La investigación policial en el ámbito de la informática”. Cuaderno del Instituto Vasco de Criminología nº 20, San Sebastián, 2006.

- JAÉN VALLEJO, MANUEL y PERRINO PÉREZ, ÁNGEL LUIS. “Recuperación de activos derivados del delito: un objetivo prioritario de la reforma penal”. Diario La Ley nº 8545, 22 de mayo de 2015.

- JEWKES YVONE y YARD MAJID (Coord). “Handbook of internet crime”. Ed. Willan Publishing, Portland USA, 2010.

- JIMÉNEZ SEGADO, CARMELO y PUCHOL AIGUABELLA, MARTA. “Las medidas de investigación tecnológica limitativas de los derechos a la intimidad, la imagen, el secreto de las comunicaciones y la protección datos”, Diario La Ley nº 8676, Sección Doctrina, 7 de enero de 2016.

- JOYANES AGUILAR, LUIS. *Introducción: Estado Del Arte De La Ciberseguridad.* En “Ciberseguridad. Retos y Amenazas a La Seguridad Nacional en el Ciberespacio”. Instituto Español de Estudios Estratégicos. Instituto Universitario General Gutiérrez-Mellado. Ministerio de Defensa, Cuaderno de estrategia nº 149. Madrid, diciembre de 2010.

- KOOPS, BERT-JAAP. *The internet and its opportunities for cybercrime* en “Transnational Criminology Manual”, Wolf Legal Publishers, Nijmegen (Holanda) 2010. http://arno.uvt.nl/show.cgi?fid=113411.

- LADRÓN DE GUEVARA JIMÉNEZ, MIGUEL ANGEL. “Sistema operativo, búsqueda de la información: Internet/Intranet y correo electrónico”. Ed. Tutor Formación, Logroño, 2014.

- LEUKFELDT, RUTGER & STOL, WOUTER (coord). "Cyber Safety: An Introduction." Ed. Eleven International Publishing. La Haya (Holanda) 2012.

- LEUKFELDT, RUTGER & DE JONG, ERIK. *Hacking* en "Cyber Safety: An Introduction." (Stol, Coord) Ed. Eleven International Publishing. La Haya (Holanda) 2012.

- LEUKFELDT, RUTGER & DE JONG, ERIK. *Basic Cybercriminal Techniques & Techniques to cause damage*. En "Cyber Safety: An Introduction." (Stol, Coord). Ed. Eleven International Publishing. La Haya (Holanda) 2012.

- LEZERTUA RODRÍGUEZ, MANUEL. *El proyecto de Convenio sobre el Cibercrimen del Consejo de Europa*, en "Internet y Derecho penal," Cuadernos de Derecho Judicial nº 10, Escuela Judicial, CGPJ, Madrid, 2001.

- LIROLA DELGADO, ISABEL. "Nuevas aportaciones al espacio de libertad, seguridad y justicia: hacia un derecho procesal europeo de naturaleza civil y penal" Revista de Derecho Comunitario Europeo nº 49, Septiembre/Diciembre 2014.

- LÓPEZ BARJA DE QUIROGA, JACOBO. "Tratado de Derecho Procesal Penal". Ed.Thomson Reuters, Aranzadi. Navarra, 2014.

- LÓPEZ JAVIER. "Insultos online, ¿soluciones offline?". Actualidad Jurídica Aranzadi nº 912, Navarra, 2015.

- LÓPEZ ORTEGA, JUAN JOSÉ. *La intimidad como bien jurídico protegido,* en Cuadernos de Derecho Judicial, volumen dedicado a "Estudios sobre el Código Penal de 1995 (parte especial)", ed. CGPJ y Escuela Judicial, Madrid, 1996.

- MACÍAS CARO, VÍCTOR MANUEL "Del orden público al terrorismo pasando por la seguridad ciudadana: análisis de las reformas de 2015". Revista Penal nº 36, 2015.

- MAEZTU LACALLE, DAVID. *La identificación del titular de una dirección IP. Problemática en aplicación de la Ley 25/2007, de conservación de datos* en "El proceso penal en la Sociedad de la Información. Las nuevas tecnologías para investigar y probar el delito" (Pérez Gil, Coord). Ed. La Ley. Madrid, 2012.

- MAGRO SERVET, VICENTE. "La delincuencia informática. ¿Quién gobierna en Internet? Diario La Ley nº 6077, 2004.

- MARCHENA GÓMEZ, MANUEL. "Dimensión jurídico-penal del correo electrónico", en Diario La Ley nº 6475, Sección Doctrina, 4 de mayo de 2006.

- MARCOS GONZÁLEZ, MARÍA. "Doctrina constitucional sobre la prueba ilícita: discrepancias interpretativas", en La Ley Penal, nº 88, Sección Estudios, Diciembre de 2011.

- MEDRANO i MOLINA, JOSEP MANEL. La práctica de la prueba por soportes informáticos y audiovisuales en el proceso penal. http://aulavirtual.uv.es/file/23588090/Prxctica_de_prueba_por_soportes.

- MESTRE DELGADO, ESTEBAN. *La cadena de custodia de los elementos probatorios obtenidos de dispositivos informáticos y electrónicos*, en "La cadena de custodia en el proceso penal", (AA.VV), Edisofer, Madrid, 2015.

- MIRANDA ESTRAMPES, MANUEL. "La prueba ilícita: la regla de exclusión probatoria y sus excepciones". Revista Catalana de Seguretat Pública. mayo 2010.

- MIRANDA ESTRAMPES, MANUEL, "La mínima actividad probatoria en el proceso penal". Ed. Bosch, Barcelona, 1997.

- MIRÓ LINARES, FERNANDO. *Cibercriminalidad y responsabilidad de los prestadores de servicios a la luz de la normativa europea y de su interpretación por los Tribunales españoles.* "Garantías constitucionales y Derecho penal europeo". Ed. Marcial Pons, Barcelona, 2012.

- MIRÓ LINARES, FERNANDO. "El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio". Ed. Marcial Pons, Barcelona, 2012. https://www.marcialpons.es/static/pdf/9788415664185.pdf

- MORALES GARCÍA, OSCAR. Delincuencia informática: intrusismo, sabotaje informático y uso ilícito de tarjetas (arts.197.3 y 8, 264 y 248), en "La Reforma Penal de 2010: Análisis y Comentarios" (Quintero Olivares, coord.) Ed. Thomson Aranzadi Reuters, Navarra, 2010.

- MORALES PRATS, FERMÍN. *Los ilícitos en la red: pornografía infantil y ciberterrorismo* En "El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas politico-criminales. (Romeo Casabona, coord.). Ed. Comares, Granada, 2006

- MORALES PRATS, FERMÍN, *Los delitos contra la intimidad en el Código Penal de 1995: reflexiones político-criminales*, en Cuadernos de Derecho Judicial, volumen dedicado a "Estudios sobre el Código Penal de 1995 (parte especial)", ed. C.G.P.J y Escuela Judicial, Madrid 1996.

- MORENILLA RODRÍGUEZ, JOSÉ MARÍA. *El derecho al respeto de la esfera privada en la jurisprudencia del Tribunal Europeo de Derechos Humanos*, en Cuadernos de Derecho Judicial, volumen dedicado a "La Jurisprudencia del Tribunal Europeo de Derechos Humanos". Ed. CGPJ, Madrid, 1993.

- MORÓN LERMA, ESTHER: "Internet y Derecho Penal: Hacking y otras Conductas Ilícitas en la Red," Colección Monografía, Ed. Aranzadi, Pamplona, Segunda edición, año 2002.

- MUERZA ESPARZA, JULIO. "Las reformas procesales penales de 2015: Nuevas medidas de agilización, de investigación y de fortalecimiento de garantías en la justicia penal". Ed. Lex nova, Navarra, 2016.

- MUÑOZ SÁNCHEZ, LORENA. *El tratamiento de los nuevos ciberdelitos en el proyecto de Código Penal*. "FODERTICS 3.0.: estudios sobre nuevas tecnologías y justícia" (Bueno de Mata coord). Ed. Comares, Granada 2015.

- NIEVA FENOLL, JORDI. "Investigaciones internas de la persona jurídica: derechos fundamentales y valor probatorio". Revista Jueces para la democracia nº 86, julio 2016.

- NIEVA FENOLL, JORDI. La recuperación de la privacidad de las comunicaciones. http://noticias.juridicas.com/conocimiento/articulos-doctrinales/11095-la-recuperacion-de-la-privacidad-de-las-comunicaciones/ 25/05/2016 10:42:29.

- NIEVA FENOLL, JORDI. "Oralidad e inmediación en la prueba: luces y sombras". Justicia: Revista de Derecho Procesal nº 1, año 2012

- NIEVA FENOLL, JORDI."Intermediación" y valoración de la prueba: el retorno de la irracionalidad". La Ley nº 7783, año 2012

- NIEVA FENOLL, JORDI. "Los sistemas de valoración de la prueba y la carga de la prueba: nociones que precisan revisión". Justicia: Revista de Derecho Procesal nº 3-4, año 2011.

- NIEVA FENOLL, JORDI. *Práctica y valoración de la prueba documental multimedia* en "Derecho y nuevas tecnología (Recurso electrónico)". Ed. Deusto, Bibao, 2010.

- NIEVA FENOLL, JORDI. "La valoración de la prueba". Ed. Marcial Pons, Madrid, 2010

NIEVA FENOLL, JORDI. "Práctica y valoración de la prueba documental multimedia". Actualidad civil nº 17, 2009.

- NIEVA FENOLL, JORDI. *La prueba en documento multimedia*, en "Instituciones del nuevo proceso civil" (AA.VV), Vol. II. Economist&Iurist, Barcelona, 2000.

- NOGALES FLORES, J. TOMÁS. Tecnologías de Internet - T1: Naturaleza y evolución de Internet. https://aulaglobal2.uc3m.es/file.php/39339/html/doc/ti/ti-01.html 02/10/2013 0:24.

- NOGALES FLORES, J. TOMÁS. Tecnologías de Internet - T2: Protocolos de Internet e identificación de equipos. https://aulaglobal2.uc3m.es/file.php/39339/html/doc/ti/ti-02.html 02/10/2013 0:26.

- ORTEGA BALANZA, MARTA y RAMÍREZ ROMERO, LUIS. "Matones en la red: cyberbullying. Tratamiento legal y respuesta jurisprudencial". Diario La Ley nº 8485, 2015.

- ORTEGA BALANZA, MARTA y RAMÍREZ ROMERO, LUIS. "De juego erótico a ciberdelito: sexting: Estudio de las respuestas legales a las problemáticas ocasionades". Iuris: Actualidad y práctica del derecho nº 221-222, 2014.

- ORTEGA GUTIÉRREZ-MATURANA, MARCELO. "Ilícitos militares cometidos a través de internet o con ocasión del uso de las nuevas tecnologías (i). Delimitación y problemas procesales y de prueba que plantean". Ponencia presentada en las Jornadas de la Fiscalía Jurídico Militar, año 2013. https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Marcelo%20Ortega%20Gutierrez-Maturana.pdf?idFile=1bf8666f-ba3e-40ae-9129-4dec942c381c.

- ORTIZ PRADILLO, JUAN CARLOS. "Problemas procesales de la ciberdelincuecia". Ed. Colex, Madrid, 2013.

- ORTIZ PRADILLO, JUAN CARLOS. "La investigación del delito en la era digital. Los derechos fundamentales frente a las nuevas medidas tecnológicas de investigación". Estudios de progreso. Fundación alternativa. 2013. http://www.fundacionalternativas.org/public/storage/actividades_descargas/5a687574bb9f245b66286372359596d4.pdf.

- ORTIZ PRADILLO, JUAN CARLOS. *Nuevas medidas tecnológicas de investigación criminal para la obtención de la prueba electrónica*, en "El proceso penal en la sociedad de la información. Nuevas tecnologías para investigar y probar el delito". (Pérez Gil, coord.). Ed. La Ley, Madrid, 2012.

- PAREDES MAZÓN, ÁNGEL. "La prevención, la investigación y enjuiciamiento los hechos ilícitos mediante grabaciones videográficas." La Ley Penal nº 89, 2012.

- PEDRAZ PENALVA, ERNESTO y ORTEGA BENITO, VICTORIA. "El principio de proporcionalidad y su configuración en la jurisprudencia del Tribunal Constitucional y literatura especializada alemanas", en Poder Judicial nº 17, Madrid, 1990.

- PÉREZ GIL, JULIO (coord.). "El proceso penal en la Sociedad de la Información. Las nuevas tecnologías para investigar y probar el delito". Ed. La Ley. Madrid, 2012.

- PÉREZ GIL, JULIO y GONZÁLEZ LÓPEZ, JUAN JOSÉ. "Cesión de datos personales para la investigación penal: una propuesta para su inmediata inclusión en la Ley de Enjuiciamiento Criminal", Diario La Ley nº 7401, 2010

- PÉREZ GIL, JULIO, "Entre los hechos y la prueba: reflexiones acerca de la adquisición probatoria en el proceso penal", Revista jurídica de Castilla y León nº 14, enero 2008.

- PÉREZ GIL, JULIO. "Investigación penal y nuevas tecnologías: algunos de los retos pendientes." Revista jurídica de Castilla y León nº 7. Derecho Procesal. Octubre 2005.

- PÉREZ GIL, JULIO. *Digitalización de la justicia y reformas procesales: un balance*, en "Estudios jurídicos sobre la Sociedad de la Información y Nuevas Tecnologías". Libro conmemorativo del XX aniversario de la Facultad de Derecho de Burgos, 2005.

- PÉREZ GIL, JULIO. *Medidas de investigación y de aseguramiento de la prueba en el convenio sobre el cibercrimen.* Homenaje a don Eduardo Font Serra. Tomo II, ed. Ministerio de Justicia, 2004.

- RIASCOS GÓMEZ, LIBARDO O. "El Derecho a la intimidad, la visión iusinformática y el delito de los datos personales". Tesis doctoral dirigida por Antonio Luis Monreal Ferrer. Universitat de Lleida (2007). http://hdl.handle.net/10803/8137.

- RÍOS PINTADO, JUAN FRANCISCO. "La reforma Procesal. Incorporación al proceso de datos de tráfico; preservación específica de datos informáticos (arts. 588 ter j y 588 octies de la LECrim)". Ponencia presentada en el curso de Formación de Fiscales

"Uso de las nuevas tecnologías y nuevas formas de delincuencia" que se celebró en el Centro de Estudios Jurídicos los días 27 al 28 de octubre de 2016. http://www.cej-mjusticia.es.

- RIVES SEVA, ANTONIO PABLO. "La prueba en el proceso penal. Doctrina de la Sala Segunda del TS". Ed. Aranzadi, sexta edición, Pamplona, 2016.

- RODRÍGUEZ LAÍNZ, JOSÉ LUIS. "Tres cuestiones polémicas sobre el registro de dispositivos electrónicos de almacenamiento masivo de información". Artículo monográfico, revista Sepín, septiembre de 2016.

- RODRÍGUEZ LAÍNZ, JOSÉ LUIS. "Sobre la naturaleza jurídica de los datos identificadores de aplicaciones de dispositivos de comunicaciones. Comentario a la STS, Sala 2.a, 551/2016". Diario La Ley nº 8831, Sección Doctrina, 26 de Septiembre de 2016.

- RODRÍGUEZ LAÍNZ, JOSÉ LUIS. "¿Podría un juez español obligar a Apple a facilitar una puerta trasera para poder analizar información almacenada en un iPhone 6?". Diario La Ley nº 8729, marzo 2016.

- RODRÍGUEZ LAÍNZ, JOSÉ LUIS. "Análisis del espectro electromagnético de señales inalámbricas: rastreo de dispositivos Wi-Fi". Diario La Ley nº 8588, Sección doctrina 2015.

- RODRÍGUEZ LAÍNZ, JOSÉ LUIS, "Aprovechamiento procesal por iniciativa policial de información recabada como consecuencia de intervención legal de comunicaciones acordada en otro proceso". Diario La Ley nº 8352, Sección doctrina 2014.

- RODRÍGUEZ LAINZ, JOSÉ LUÍS. "La interceptación de las comunicaciones telefónicas y telemáticas en el Anteproyecto de reforma de la Ley de Enjuiciamiento Criminal de 5 de diciembre de 2014". Diario La Ley nº 8465, Sección doctrina 2015.

- RODRÍGUEZ LAINZ, JOSÉ LUÍS. "GPS y balizas policiales". Diario La Ley nº 8416, 2014.

- RODRÍGUEZ LAINZ, JOSÉ LUÍS. "Reflexiones sobre los nuevos contornos del secreto de las comunicaciones (Comentario a la STC 170/2013, de 7 de octubre)". Diario La Ley nº 8271, 2014.

- RODRÍGUEZ LAINZ, JOSÉ LUÍS. "Sobre la incidencia de la declaración de invalidez de la Directiva 2006/24/CE en la ley española sobre conservación de datos relativos a las comunicaciones". Diario La Ley nº 8308, Sección Doctrina, 2014.

- RODRÍGUEZ LAÍNZ, JOSÉ LUIS, "De vueltas con SITEL". Diario La Ley nº 7515, Sección doctrina 2010.

- RODRÍGUEZ-MEDEL NIETO, CARMEN. "Obtención de la admisibilidad en España de la prueba penal transfronteriza". Ed. Aranzadi, Navarra, 2016

- RODRIGUEZ MOURULLO, GONZALO; ALONSO GALLO, JAIME; LASCRUAN SANCHEZ, JUAN ANTONIO. *Derecho penal e Internet*, en "Régimen jurídico de internet", la ley-Actualidad 2002.

- RODRÍGUEZ NÚÑEZ, ALICIA. *Prueba y Proceso Penal* en "Fundamentos de la investigación criminal". Instituto Universitario General Gutiérrez Mellado. UNED. Madrid. 2008. http://iugm.es/uploads/tx_iugm/FUNDAMENTOS__INV__CRIM_01.pdf

- ROMEO CASABONA, CARLOS MARÍA. *De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal*, en "El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales" (Romeo Casabona, Coord). Ed. Comares, Granada, 2006.

- ROMEO CASABONA, CARLOS MARÍA. *Los datos de carácter personal como bienes jurídicos penalmente protegidos*, en "El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político- criminales" (Romeo Casabona, Coord). Ed. Comares, Granada, 2006.

- ROMEO CASABONA, CARLOS MARÍA. "La protección penal de los mensajes de correo electrónico y de otras comunicaciones de carácter personal a través de internet". Revista Aranzadi de derecho y nuevas tecnologías nº 10, 2006.

- ROMERO PAREJA, AGUSTÍN. "Intervención de las comunicaciones". Diario La Ley nº 7816, Sección Doctrina, marzo 2012.

- ROVIRA DEL CANTO, ENRIQUE. "Nuevas formas de ciberdelincuencia intrusiva: el hacking y el grooming". Iuris: Actualidad y praáctica de derecho nº 160, 2011.

- ROVIRA DEL CANTO, ENRIQUE. "Las nuevas pruebas telemáticas y digitales. especialidades de la prueba en delitos cometidos por internet". Estudios Jurídicos. Ministerio Fiscal (vol. I), 2003.

- ROVIRA DEL CANTO, ENRIQUE. "Hacia una expansión doctrinal y fáctica del fraude informático". Revista Aranzadi de derecho y nuevas tecnologías, nº 2003-3, año 2003.

- ROVIRA DEL CANTO, ENRIQUE. "Delincuencia Informática y fraudes informáticos". Ed. Comares, Granada, 2002.

- ROVIRA DEL CANTO, ENRIQUE. *Tratamiento penal sustantivo de la falsificación informática.* Cuadernos de derecho judicial nº 10, ejemplar dedicado a "internet y derecho penal", 2001

- RUBIO ALAMILLO, JAVIER. "Consevación de la cadena de custodia de una evidencia informática". Diario La Ley nº 8859, Sección Doctrina, 9 de Noviembre de 2016.

- RUBIO ALAMILLO, JAVIER. "La informática en la reforma de la Ley de Enjuiciamiento Criminal". Diario La Ley nº 8662, Sección Tribuna, 10 de diciembre de 2015.

- RUBIO ALAMILLO, JAVIER. "La dirección IP en el peritaje informático". Abril de 2015. http://peritoinformaticocolegiado.es/la-direccion-ip-en-el-peritaje-informatico/. 18/2/2016 a las 20.19 horas.

- RUBIO ALAMILLO, JAVIER. "El Tribunal Supremo dictamina que un perito informático debe autentificar las conversaciones mantenidas a través de una red social". Mayo de 2015. http://peritoinformaticocolegiado.es/el-tribunal-supremo-dictamina-que-un-perito-informatico-debe-autentificar-conversaciones-mantenidas-red-social/ 18/2/2016 a las 21.05 horas.

- RUBIO ALAMILLO, JAVIER. "Peritaje informático de correos electrónicos". Diciembre de 2014. http://peritoinformaticocolegiado.es/peritaje-informatico-de-correos-electronicos/ 18/2/2016 a las 21.13 horas.

- RUBIO ALAMILLO, JAVIER. "Clonación de discos duros en el peritaje informático". Junio 2014. http://peritoinformaticocolegiado.es/clonacion-de-discos-duros-en-el-peritaje-informatico/ 18/ 2/2016 a las 20.35 horas.

- RUBIO ALAMILLO, JAVIER. "El perito informático y el rastro en Internet y las redes sociales. Octubre de 2014. http://peritoinformaticocolegiado.es/el-perito-informatico-y-el-rastro-en-internet-y-las-redes-sociales/ 18/2/2016 a las 20.46 horas.

- RUBIO ALAMILLO, JAVIER. "Peritaje informático de conversaciones de WhatsApp o aplicaciones similares". Septiembre 2014. http://peritoinformaticocolegiado.es/peritaje-informatico-de-conversaciones-de-whatsapp-o-aplicaciones-similares/ 18/2/2016 a las 20.49 horas.

- RUIZ VADILLO, ENRIQUE. "Estudios de Derecho Procesal Penal". Ed. Comares, Granada, 1995.

- SÁNCHEZ BRAVO, ALVARO A. "El convenio del Consejo de Europa sobre cibercrimen: control vs. libertades públicas". La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía nº 3, 2002.

- SÁNCHEZ DOMINGO, MARÍA BELÉN. "La Cooperación Judicial Penal y el Tratado de Lisboa. El ejemplo de La Directiva 2011/92/Ue en materia de pornografía Infantil". Revista de derecho comunitario europeo nº 44. Madrid, enero/abril (2013). dialnet.unirioja.es/descarga/articulo/4320147.pdf

- SÁNCHEZ LINDE, MARIO. *Las conductas del artículo 248.2.b del código penal como delito de estafa informática.* En "Fraude electrónico: su gestión penal y civil". Ed. Tirant lo Blanch, Valencia, 2015.

- SÁNCHEZ MEDERO, GEMA. "Internet: un espacio para el cibercrimen y el ciberterrorismo". Crisis analógica, futuro digital: actas del IV Congreso Online del Observatorio para la Cibersociedad, celebrado del 12 al 29 de noviembre de 2009.

- SÁNCHEZ SISCART, JOSÉ MANUAL. "Cibercrimen y cooperación judicial. Especial referencia a los ISP alojados en EE.UU." Revista Poder Judicial nº 91, quinta época año 2011. Foro de opinion.

- SÁNCHEZ SISCART, JOSÉ MANUEL. "A vueltas con el secreto de las comunicaciones: algunos supuestos críticos en la jurisprudencia de la Sala 2ª del Tribunal Supremo". Diario La Ley nº 7338, Sección Doctrina, 9 de febrero de 2010.

- SANCHÍS CRESPO, CAROLINA. en *La prueba en soporte electrónico*, dentro de la obra colectiva "Las Tecnologías de la Información y de la Comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio" (Gamero Casado y Valero Torrijos, coord.). Ed. Thomson Reuters Aranzadi, Navarra, 2012.

- SANDYWELL, BARRY. *On the globalisation of crime: the internet and new criminality*. En "Handbook of internet crime". (Yvone Jewkes and Majid Yard, coord.). Ed. Willan Publishing, Portland USA, 2010.

- SMITH RUSSEL G, GRABOSKY PETER, URBAS GREGOR. "Cyber Criminals on Trial". Ed. Cambridge University Press. Cambridge, 2011.

- STOL, WOUTER. *Cyberspace and safety*. En "Cyber Safety: An Introduccion". (Stol Coord). Ed. Eleven International Publishing. Holanda, 2012.

- TAMARIT SUMALLA, JOSEP MARÍA. "Crónica de la III Jornada de Criminología UOC-CEFJE: Ciberdelito y Victimización". Revista de Internet, derecho y política nº 16, 2013 (Ejemplar dedicado a: Regulación de la delincuencia en Internet).

- TEJADA DE LA FUENTE, ELVIRA. *La retención obligatoria de datos de tráfico de las comunicaciones electrónicas y telemáticas y la preservación específica de datos*

informáticos como herramientas de investigación criminal en "El Derecho de Internet" (Pérez Bes, Coord). Ed. Atelier, Barcelona, 2016.

- TEJADA DE LA FUENTE, ELVIRA. "Aproximación a las herramientas de investigación tecnológica en el proyecto de reforma procesal en curso". Ponencia presentada en la jornada sobre violencia de genero especial referencia a nuevas tecnologias, 2015. www.cej-mjusticia.es.

- TEJADA DE LA FUENTE, ELVIRA. "Problemas generales en la investigación de la criminalidad informática". Ponencia presentada en el curso Menores e Internet año. 2012.www. cej.mjusticia.es.

- TEJERINA RODRÍGUEZ, OFELIA. "El registro remoto de equipos informáticos" en http://www.internautas.org/html/8833.html.

- THOMAS, DOUGLAS y LOADER, BRIAN. "Cybercrime: law enforcement, security and surveillance in the information age". Ed. Cambridge University Press. Routledge, London, 2000.

- URÍA GAVILÁN, ELISA. "Derechos fundamentales versus vigilancia masiva. Comentario a la sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015 en el asunto C-362/14 *Schrems*". Revista de Derecho Comunitario Europeo nº 53, 2015.

- URIARTE VALIENTE, LUIS M. "Algunos pronunciamientos jurisprudenciales sobre la intervención de comunicaciones telefónica". Ponencia presentada en el curso de formación continua de Fiscales del año 2016, sobre La interceptación de las comunicaciones telefónicas y telemáticas, celebrada en Madrid del 27/4/2016 al 29/04/2016. http://www.cej-mjusticia.es.

- VALLÉS CAUSADA. LUIS M. *Usos delictivos no comunicativos de la telefonía móvil: ¿una excepción a la protección del artículo 18.3 CE?* en "El proceso penal en la

Sociedad de la Información. Las nuevas tecnologías para investigar y probar el delito"(Pérez Gil, Coord). Ed. La Ley. Madrid, 2012.

- VAN EEKELEN, MARKO (M.C.J.D) & VRANKEND, HARALD (HPE). *The Internet: Historical and Technical Background*, en"Cyber Safety: An Introduccion" (Stol Coord). Ed. Eleven International Publishing. Holanda, 2012.

- VALIÑO CES, ALMUDENA. "Una lectura crítica en relación al agente encubierto informático tras la Ley Orgánica 13/2015". Diario La Ley nº 8731, 30 de Marzo de 2016.

- VALMAÑA CABANES, ANTONIO. "La validez probatoria de los correos electrónicos: lo escrito, escrito está". www.legaltoday.com. Práctica jurídica.

- VALVERDE MEGÍAS, ROBERTO. "Intervención de comunicaciones telemáticas y registro remoto". Ponencia presentada en el curso de Formación de Fiscales "Uso de las nuevas tecnologías y nuevas formas de delincuencia" que se celebró en el Centro de Estudios Jurídicos los días 27 al 28 de octubre de 2016.

- VÁZQUEZ SECO, LUIS. "Incorporación de datos al proceso. Vigencia de la Ley 25/2007 de 18 de octubre de conservación de datos relativos a las comunicaciones electrónicas y redes públicas e interpretación de la Ley a la luz de la reforma operada por LO 13/2015". Ponencia presentada en el curso de Formación de Fiscales "Uso de las nuevas tecnologías y nuevas formas de delincuencia" que se celebró en el Centro de Estudios Jurídicos los días 27 al 28 de octubre de 2016.

- VELASCO NÚÑEZ, ELOY. "Delitos tecnológicos: definición, investigación y prueba en el proceso penal". Ed. Sepín. Madrid, 2016.

- VELASCO NÚÑEZ, ELOY. "Novedades técnicas de investigación penal vinculadas a las nuevas tecnologías", Revista de Jurisprudencia el derecho nº 4, febrero de 2011.

- VELASCO NÚÑEZ, ELOY. "Delitos cometidos a través de Internet. Cuestiones Procesales". La Ley- Actualidad, Madrid, 2010.

- VELASCO NÚÑEZ, ELOY. "Delitos informáticos, terrorismo y derecho internacional en el anteproyecto de Ley Orgánica 2008, por la que se modifica la Ley Orgánica 10/1995, del Código Penal". La Ley Penal: revista de derecho penal, procesal y penitenciario nº 63, 2009.

- VELASCO NÚÑEZ, ELOY. "Los delitos informáticos: especial referencia a la pornografía infantil". Cuadernos Digitales de Formación nº 22, 2009.

- VELASCO SAN MARTÍN, CRISTOS. "Jurisdicción y competencia penal en relación al acceso transfronterizo en materia de ciberdelitos". Ed. Tirant lo Blanch, Valencia, 2016.

- VERDEJO ESPINOSA, Mª ÁNGELES. "Ciberacoso y violencia de género en redes sociales: análisis y herramientas de prevención". Universidad Internacional de Andalucía, 2015.

- VILLACAMPA ESTIARTE, CAROLINA y GÓMEZ ADILLÓN, Mª JESÚS. "Nuevas tecnologías y victimización sexual de menores por Online Grooming". Revista Electrónica de Ciencia Penal y Criminología nº 18-02, 2016.

- VILLACAMPA ESTIARTE, CAROLINA. "Propuesta sexual telemática a menores u online child grooming: configuración presente del delito y perspectivas de modificación". Revista Estudios penales y criminológicos Vol. 34, 2014.

- VILLAGÓMEZ MUÑOZ, ANA. "Otras medidas de investigación limitativas de derechos reconocidos por el art. 18 C.E. referencia concreta a los dispositivos de seguimiento y localización". Ponencia presentada en el curso de formación continua de Fiscales del año 2016, sobre La interceptación de las comunicaciones telefónicas y telemáticas, celebrada en Madrid del 27/4/2016 al 29/04/2016. http://www.cej-mjusticia.es.

- VILLEGAS GARCÍA, MARÍA ÁNGELES. "La utilización de dispositivos de geolocalización en el proceso penal. El estado de la cuestión en la Jurisprudencia Federal de los Estados Unidos." en Revista de Derecho y Proceso Penal nº 42, 2016.

- VILLODRE LÓPEZ, JOSÉ. "Los Equipos Conjuntos de Investigación (JIT)". Ponencia presentada el día 20 de abril de 2016 en las IV Jornadas de Derecho Procesal organizadas por la 7ª Zona de la Guardia Civil de Catalunya, Sobre Cooperación Judicial Penal.

- WALL, DAVID S. *Criminalising cyberspace: the rise of the internet as a crime problem.* En "Handbook of internet crime". (Yvone Jewkes and Majid Yard, coord.). Ed. Willan Publishing, Portland USA, 2010.

- WALL, DAVID S. "Cybercrime: The transformation of crime in the information age". Ed. Cambridge, polity press, UK, 2007.

- YAR MAJID. "The Novelty of 'Cybercrime" European Society of Criminology and SAGE Publications London, Thousand Oaks CA, and New Delhi, 2005.

- ZARAGOZA TEJADA, JAVIER IGNACIO. "La reforma operada por Ley 13/2015. El Agente Encubierto Informático". Ponencia presentada en el curso de Formación de Fiscales "Uso de las nuevas tecnologías y nuevas formas de delincuencia" que se celebró en el Centro de Estudios Jurídicos los días 27 al 28 de octubre de 2016. http://www.cej-mjusticia.es.

- ZOCO ZABALA, CRISTINA. "Interceptación de las comunicaciones electrónicas". Concordancias y discordancias de SITEL con el artículo 18 CE. InDret, revista para el análisis del derecho. Barcelona, octubre 2010. http://www.indret.com/pdf/781_es.pdf

- "Los delitós informáticos". Departamento jurídico de Sepín Penal. Noviembre de 2016.

-VV.AA. "La prueba en el Proceso Penal". Ed. Thomson-Reuters. 2016.

- "Ciberacoso: los delitos de acoso a través de internet y de medios de comunicación electrónica". Departamento jurídico de Sepín Penal. Noviembre de 2016.

- Memoria de la Fiscalía General del Estado 2016 en materia de criminalidad informática.

- La Sociedad de la Información en España 2015_siE[13". Fundación Telefónica. Ed. Ariel, Barcelona, 2016. http://www.fundacion.telefonica.com/es/arte_cultura/publicaciones/detalle/258.

- Circular 8/2015 sobre los delitos contra la propiedad intelectual cometidos a través de los servicios de la sociedad de la información.

- Estudio sobre la cibercriminalidad en España, año 2015. Ministerio del Interior. Secretaría de Estado de Seguridad. Gabinete de Coordinación y Estudios.

- Conclusiones de la II jornada sobre el marco jurídico de actuación del agente encubierto (Madrid, 29 de mayo de 2015). Ministerio de Justicia. ANEXO: Conclusiones refundidas (I y II Jornadas sobre Marco Jurídico del Agente Encubierto).

- Memoria de la Fiscalía General del Estado 2015 en materia de criminalidad informática.

- "El fraude informático es el principal ciberdelito en España". Revista SIC: ciberseguridad, seguridad de la información y privacidad nº 111, 2014.

- Informe del Consejo Fiscal en relación con la problemática relativa a los Equipos Conjuntos de Investigación, Madrid 23 de julio de 2014.

- Manual de buenas prácticas sobre firma electrónica. Dirección de Sistemas de Información Departamento Ceres. Editado por CERES, en 2007, última revisión 2014. http://www.cert.fnmt.es/documents/11614/75209/Manual+de+Buenas+Prácticas/b7680a65-f04c-4138-bca6-892f458b6c25.

- Circular de la Fiscalía General del Estado 1/2013 sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas.

- Circular de la Fiscalía General del Estado 4/2013 sobre las Diligencias de Investigación.

- "Estrategia Europea de Ciberseguridad". Apuesta de la UE por las unidades nacionales de lucha contra el ciberdelito y el desarrollo de estándares para productos y Servicios Revista SIC: ciberseguridad, seguridad de la información y privacidad, nº. 104, 2013.

- Estrategia de Ciberseguridad Nacional. Departamento de Seguridad nacional. Presidencia del Gobierno, 2013.

- La prueba electrónica en el proceso judicial. Ventajas e inconvenientes". Facultad de Derecho. Departamento de Criminología: Universidad de Málaga. 15 marzo de 2013. www.uma.es/criminología/pdf/ponencias.

- *"Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations"* 2009. https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf

- Dirección de Sistemas de Información Departamento Ceres. Firma Electrónica De Larga Duración. Firma Longeva. Editado por CERES, en 2008. http://www.cert.fnmt.es/documents/11601/94960/Firmas_longevas.pdf/1461fea7-64a8-4b27-8cdd-9f31f40f5f0c.

- "IPV6 Aspectos Legales del nuevo protocolo de Internet". Euro6ix. Comisión Europea. http:// ipv6tf.org.