Fernández González, F.C., Fuentes García Romero de Tejada, C., González Manzano, L., Fuentes García Romero de Tejada, J.M. (2021). Revisión sistemática de la jurisprudencia española sobre ciberseguridad y privacidad (1995- 2020). *Revista de privacidad y derecho digital*, VI(24), pp. 144-190.

REVISIÓN SISTEMÁTICA DE LA JURISPRUDENCIA ESPAÑOLA SOBRE CIBERSEGURIDAD Y PRIVACIDAD (1995-2020) (*) [1]

ON THE CYBERSECURITY -AND PRIVACY- RELATED CASES IN THE SPANISH HIGHER COURTS: A SYSTEMATIC REVIEW

Por FERNANDO CÉSAR FERNÁNDEZ GONZÁLEZ
Banco de España.

Por CARLOS DE FUENTES Gª-ROMERO DE TEJADA
Profesor Asociado Derecho del Trabajo y de la Seguridad Social, UCM.

Por LORENA GONZÁLEZ MANZANO
Profesora Titular Seguridad Informática, UC3M.

Por JOSÉ MARÍA DE FUENTES Gª-ROMERO DE TEJADA
Profesor Titular Seguridad Informática, UC3M.

1 Este trabajo se enmarca en el Proyecto de la Comunidad de Madrid (España) CYNAMON, subvención nº P2018/TCS-4566-CM, cofinanciado con FEDER, y también ha sido apoyado por la Universidad Carlos III de Madrid (España), Subvención CAVTIONS-CM-UC3M y por el proyecto "El futuro del trabajo: transformaciones y retos", Universidad Complutense de Madrid (España), Ref.970922.

(*) Este trabajo se recibió en mayo de 2021 y fue admitido en junio de 2021

RESUMEN

La expansión de las tecnologías de la información y la comunicación y el aumento de la conectividad, ha provocado el surgimiento de una gran cantidad de delitos como el *grooming* o la suplantación de identidad, por citar algunos. Sin embargo, no se ha evaluado la relevancia de esta materia en los tribunales españoles. Para superar esta limitación, en este trabajo realizamos un análisis sistemático de la jurisprudencia emanada bien del Tribunal Supremo, bien del Tribunal Constitucional, a través de 117 resoluciones desde 1995 hasta 2020. Nuestro análisis muestra las cuestiones jurídicas que son más frecuentes y revisa cómo han ido evolucionando los diversos conceptos jurídicos sobre ciberseguridad y privacidad.

PALABRAS CLAVE. *Ciberseguridad; Privacidad; Protección de Datos; Autenticación; Tribunales españoles; Jurisprudencia.*

ABSTRACT

With the explosion of information and communication technologies and the increase of connectivity, a plethora of offences have been identified such as grooming, personal data protection or impersonation, to name a few. Nevertheless, the relevance of this matter in Spanish courts has not been assessed. To overcome this limitation, in this paper we carry out a systematic analysis on 117 resolutions from 1995 to date. All of them belong to the Spanish Higher Courts, namely the Supreme Court and the Constitutional Court. This is particularly relevant as their resolutions can set a precedent that has to be observed by lower courts. Our analysis shows the legal issues that are more often at stake as well as the trends in terms of legal doctrines and punishments.

KEY WORDS: *Cybersecurity; Citizens privacy; Data security; Citizens authentication; Spain; Resolution; Higher Courts.*

SUMARIO

I.- INTRODUCCIÓN

En los últimos años, las sociedades modernas han sido testigos de un aumento en la importancia de cuestiones tecnológicas que tienen impacto en la vida diaria. Una muestra de ello es el incremento exponencial de dispositivos informáticos conectados[1]. Junto con la explosión de dispositivos, la conectividad también ha aumentado en los países desarrollados por lo que se puede concluir que el uso ubicuo de ordenadores y dispositivos relacionados es una realidad para la gran mayoría de la población. En consonancia con esta tendencia, la cantidad de delitos informáticos también ha aumentado. Así, se ha acuñado el término ciberdelincuencia, que puede definirse como "el uso de un ordenador como instrumento para conseguir fines ilegales, como cometer fraudes, traficar con pornografía infantil y propiedad intelectual, robar identidades o violar la privacidad"[2]. De hecho, según un informe del Parlamento Europeo, la ciberdelincuencia denunciada supera a la tradicional en algunos países de la UE[3].

La persecución de los ciberdelitos requiere una preparación adecuada desde el punto de vista jurídico. Esta cuestión es de máxima relevancia en España, que es el país protagonista para esta investigación. La reciente Estrategia Española de Ciberseguridad 2019 cuenta con una línea de actuación a medida en este sentido ("reforzar las capacidades de investigación y persecución de la ciberdelincuencia, para garantizar la seguridad ciudadana y proteger los derechos y libertades en el ciberespacio"), que tiene una medida asociada que es el núcleo de este trabajo: "obtener el acceso a la información y a los recursos materiales de los operadores jurídicos que garanticen una mejor aplicación del marco jurídico y técnico de lucha contra la ciberdelincuencia, dotándoles de mayores capacidades para investigar y juzgar los correspondientes ilícitos"[4].

1 Por ejemplo, en 2019 se vendieron 1.520 millones de smartphones. Toda la información sobre el número de este tipo de terminales vendidos desde 2007 está accesible en https://www.statista.com/statistics/263437/global-smartphone-sales-to-end-users-since-2007/

2 Según la Enciclopedia Británica, https://www.britannica.com/topic/cybercrime

3 Resolución del Parlamento Europeo, de 3 de octubre de 2017, sobre la lucha contra la ciberdelincuencia (2017/2068 (INI)).

4 https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019

Más allá de los ciberdelitos, la mera utilización de medios informáticos (como ordenadores, dispositivos o unidades de almacenamiento) supone la aparición de nuevas circunstancias que deben ser analizadas a la hora de juzgar casos no informáticos. Por ejemplo, cuando los documentos se almacenan en un CD-ROM, pueden entrar en juego derechos fundamentales como el del secreto de las comunicaciones. Además, la integridad o la autoría de estos documentos puede ponerse en tela de juicio y socavar su potencial para servir de prueba. En general, estas cuestiones relacionadas con la informática pueden referirse a la seguridad de los datos y a la autentificación y privacidad de los ciudadanos.

Tanto los ciberdelitos como el resto de cuestiones relacionadas con la informática son los principales ingredientes de un concepto relativamente nuevo: la ciberseguridad. Aunque no existe una definición mundial de este concepto, puede describirse como "la protección de los sistemas y redes informáticos contra el robo o el daño de su hardware, software o datos electrónicos, así como contra la interrupción o el desvío de los servicios que proporcionan"[5]. En este trabajo optamos por esta definición, ya que incluye las tres nociones relevantes introducidas anteriormente: los ciberdelitos, los problemas de seguridad de los datos y las consideraciones de autenticación y privacidad de los ciudadanos. Esto coincide con la perspectiva del gobierno español. Hay que tener en cuenta que España cuenta con un Código de leyes de ciberseguridad que es actualizado regularmente por el Instituto Español de Ciberseguridad (INCIBE)[6], esfuerzo compilador para incluir las diferentes normas que tienen alguna relación con las tres nociones mencionadas.

Para conocer una disciplina jurídica, además de los textos legales, es conveniente observar la forma en que están siendo aplicados y entendidos por los jueces y otros profesionales del derecho. Por ello, además del Código legislativo antes indicado, es preciso dominar la jurisprudencia emanada de los Altos Tribunales de nuestro ordenamiento jurídico, a saber, el Tribunal Supremo y el Tribunal Constitucional, que están habilitados para sentar precedentes de

5 https://dbpedia.org/page/Computer_security

6 https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=173_Codigo_de_Derecho_de_la_Ciberseguridad&modo=2

interpretación de las normas que deben ser considerados por los tribunales inferiores (art. 1.6 Código Civil y 5.1 Ley Orgánica del Poder Judicial).

En trabajos anteriores ya se ha puesto de manifiesto el reto legal que los asuntos de ciberseguridad suponen para los profesionales del derecho. En particular, Mallada Fernández[7] y Bernárdez Cabello[8] son los principales precedentes en la dirección de esta investigación. Ambos trabajos han estudiado algunos delitos informáticos desde una perspectiva jurídica. Sin embargo, hasta donde los autores saben, no existe ningún trabajo previo que ofrezca una visión general de la comprensión y aplicación de estas leyes en casos relacionados con la ciberseguridad en los Tribunales Constitucional y Supremo de España.

En efecto, son pocos los trabajos que han abordado las cuestiones jurídicas relacionadas con la ciberseguridad. Por un lado, Jimeno[9] propuso una taxonomía exhaustiva sobre los diferentes derechos y bienes que pueden verse afectados por la informática. No obstante, en el enfoque de su trabajo la evolución legislativa y jurisprudencial no tiene la importancia que nosotros hemos querido poner de relieve.

El análisis sobre la evolución de las leyes en materia de ciberseguridad es realizado por Davara Fernández de Marcos[10], con especial énfasis en los ciberdelitos y en materia de privacidad en las redes sociales. A diferencia de nuestro trabajo, su análisis no se centra en la aplicación de las leyes en las resoluciones judiciales. Hay que tener en cuenta que esta aplicación y la interpretación subyacente es esencial para entender el significado práctico de las nociones de ciberseguridad.

7 AA.VV. (MALLADA FERNÁNDEZ, C., Coord.)**,** *Nuevos retos de la ciberseguridad en un contexto cambiante,* Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2019.

8 BERNÁNDEZ CABELLO, O., RAMOS-PAÚL DE LASTRA, I., *Retos de la tutela judicial efectiva frente a las ciberamenazas. Retos del derecho ante las nuevas amenazas*, Dykinson, Madrid, 2015, págs. 111-123.

9 JIMENO MUÑOZ, J., *Derecho de daños tecnológicos: ciberseguridad e insurtech*, Dykinson, Madrid, 2019.

10 DAVARA FERNÁNDEZ DE MARCOS, E. y DAVARA FERNÁNDEZ DE MARCOS, L., *Delitos Informáticos*, Aranzadi, Cizur Menor (Navarra), 2017.

Hasta donde los autores saben, sólo una tesis doctoral pone el foco en las sentencias judiciales[11]. Sin embargo, su alcance se limita a los ciberdelitos relacionados con el terrorismo y se limita a siete resoluciones. En este sentido, nuestro trabajo es más amplio tanto en la cantidad de resoluciones en juego como en las ramas del ordenamiento jurídico consideradas.

Para superar esta limitación, en este trabajo pretendemos analizar la evolución de las resoluciones relacionadas con la ciberseguridad en los más Altos Tribunales españoles (Supremo y Constitucional). El reto jurídico subyacente es, por tanto, desvelar cómo estos Tribunales están entendiendo las cuestiones de ciberseguridad y aplicando la normativa existente en consecuencia. La relativa novedad de algunos delitos informáticos (por ejemplo, la suplantación de identidad, el *grooming*, la denegación de servicio, etc.) puede dar lugar a diferentes interpretaciones, por lo que pretendemos aclarar cuáles son las principales nociones y fundamentos que se observan en las resoluciones que pueden ser interesantes para todos los operadores jurídicos que se enfrentan a asuntos relacionados con la ciberseguridad.

El trabajo lo hemos estructurado de la siguiente manera. En el apartado segundo explicamos la metodología utilizada para la obtención de la selección de las sentencias y se describirá el conjunto de resoluciones identificadas. A partir del apartado tercero, se irán analizando, por materias, dichas sentencias. Así, comenzaremos con la interpretación de normas constitucionales (apartado 3); ámbito penal (apartado 4); jurisprudencia sobre protección de datos (apartado 5); asuntos procesales (apartado 6) y laborales (apartado 7), para concluir, en el punto octavo, con las conclusiones y posibles futuros trabajos. En el anexo ofrecemos el listado de sentencias seleccionadas, base de nuestra investigación y un resultado de interés para la comunidad científica y los profesionales del Derecho.

11 ONS GAMON, V., *Ciberterrorismo amenaza a la seguridad. Respuesta operativa y legislativa, nacional e internacional*, Tesis Doctoral (inédita), Universidad Nacional de Educación a Distancia (UNED), 2018, accesible en línea: http://e-spacio.uned.es/fez/eserv/tesisuned:ED-Pg-DeryCSoc-Vpons/PONS_GAMON__Vicente_Tesis.pdf

II.- METODOLOGÍA UTILIZADA PARA LA OBTENCIÓN DE LA SELECCIÓN DE SENTENCIAS

Los autores seleccionaron primeramente 177 sentencias de los Tribunales Constitucional y Supremo que contenían las voces de ciberseguridad, seguridad informática, privacidad o "phishing". De ellas, finalmente se identificaron 117 cuya temática versaban sobre las materias objeto de estudio y, por tanto, eran idóneas para la finalidad de la investigación. Sólo cinco son del Tribunal Constitucional y el resto (112) corresponden al Supremo. No obstante, la trascendencia del ámbito constitucional, implicación de los Derechos Fundamentales afectados, es muy relevante como luego veremos con detalles.

Como antes se comentó, en el anexo se ofrece el listado de sentencias seleccionadas, base de nuestra investigación y que, sin duda, desde nuestro punto de vista, supone un resultado de interés para la comunidad científica y los profesionales del Derecho (judicatura, abogacía, administración y empresas) que se relacionan con el campo de la informática.

El conjunto de resoluciones idóneas escogidas se reparte en un lapso de tiempo entre 2007 y 2020 (Fig. 1). Entre 1995 y 2007 se encontró una cantidad muy reducida de decisiones, lo cual es lógico por la menor trascendencia que tenía en esa época. Así pues, el conjunto de datos considerado refleja con exactitud las tendencias jurídicas de los últimos 13 años (2007-2020).

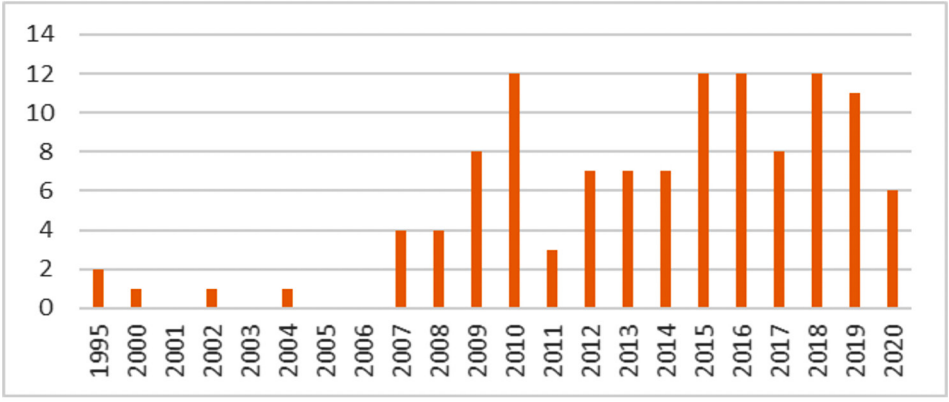

Fig. 1. Cronología de las sentencias estudiadas (elaboración propia).

En lo que se refiere a qué parcela del ordenamiento jurídico está en juego, la Figura 2 muestra la distribución. La mayor parte de los casos están relacionados con cuestiones penales (73%), aunque los asuntos contencioso-administrativos también están notablemente presentes (17%). Por último, los asuntos sociales son tratados sólo en seis decisiones y un único caso en la Sala de lo Militar.

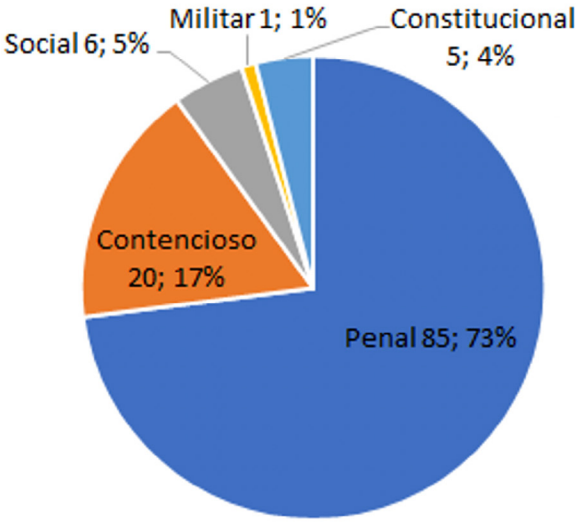

Fig. 2. Distribución por rama del Ordenamiento Jurídico (elaboración propia).

III.- JURISPRUDENCIA CON RELEVANCIA CONSTITUCIONAL SOBRE CIBERSEGURIDAD (DERECHOS FUNDAMENTALES IMPLICADOS Y REPARTO COMPETENCIAL ENTRE ADMINISTRACIONES)

En este apartado se explica cómo los tribunales Supremo y Constitucional han interpretado los artículos de la Constitución Española referidos a la protección de los Derechos Fundamentales a la intimidad, a la inviolabilidad del domicilio, al derecho al secreto de las comunicaciones y a la protección de datos y a la libertad informática, siempre sobra la base de la doctrina de las sentencias

recuperadas en nuestra investigación. Asimismo, se dedica un epígrafe concreto al tratamiento jurisprudencial del reparto constitucional de competencias en materia de ciberseguridad (Estado-Comunidades Autónomas).

1. DERECHO A LA INTIMIDAD (ART. 18.1 CONSTITUCIÓN ESPAÑOLA)

El artículo 18.1 de la Constitución Española (en adelante, CE) establece que "se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen" como un derecho fundamental. En nuestra investigación hemos recuperado veinte resoluciones en las que el Tribunal Supremo examina este precepto constitucional en asuntos de seguridad informática, en todos los casos aplicable junto a otros preceptos constitucionales como los referidos a la protección del derecho al secreto de las comunicaciones o a la protección de datos y a la libertad informática, cuyo tratamiento jurisprudencial veremos más adelante.

En materia de vulneración del derecho a la intimidad en relación con la seguridad informática, destacamos una serie de sentencias de la Sala de lo Penal del Tribunal Supremo en las que además de enjuiciarse determinados delitos informáticos, se declara en todos los casos que se ha producido la vulneración del derecho a la intimidad de las víctimas; en este sentido se pronuncian las sentencias de 8 de febrero de 2018 y de 24 de febrero de 2015 sobre abuso informático a menores; las sentencias de 2 de marzo y 21 de junio de 2016 y 19 de diciembre de 2019, sobre delito de descubrimiento y revelación de secretos.

Un segundo aspecto interesante de las resoluciones analizadas versa sobre la acotación de los términos de privacidad e intimidad, otorgando el Tribunal Supremo al primero un ámbito de aplicación más amplio, referido a la protección de datos personales, y reservando el término "intimidad" a la esfera más íntima de la persona. En este sentido, destacamos la sentencia del Tribunal Supremo de 5 de junio de 2009[12] que declara que "pues en tanto ésta (la intimidad) protege

12 STS 5-06-2009. Rec. 2295/2008. https://www.poderjudicial.es/search/AN/openDocument/0a95cb45da20e8a0/20090716

la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona, la privacidad constituye un conjunto más amplio, más global, de facetas de su personalidad que aisladamente consideradas pueden carecer de significación intrínseca pero que coherentemente enlazadas entre sí arrojan un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado". La diferenciación entre ambos conceptos se discutió en el caso de un funcionario al que se le intervino un CD con documentación falsificada en el registro de su mesa de trabajo, sin que tal documentación, rotulada en el CD como "expedientes administrativos" pueda afectar a la intimidad de la persona, aunque sea de carácter privado. En similares términos se pronuncia la sentencia del Tribunal Supremo (Penal) de 11 de junio de 2004[13], estableció que "el registro de la mesa de un funcionario: no vulnera su derecho a la intimidad, porque el lugar de trabajo de funcionarios que tienen el deber de custodiar la privacidad de los administrados no constituye un ámbito de privacidad del funcionario"

2.- SOBRE LA INTERPRETACIÓN DE LA INVIOLABILIDAD DEL DOMICILIO (ART. 18.2 CE)

El artículo 18.2 CE declara que "el domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito".

En el ámbito de la seguridad informática, hemos recuperado una serie de once sentencias en las que el Tribunal Supremo se ha pronunciado sobre la inviolabilidad del domicilio referido a la entrada en las instalaciones de una empresa y a registro de equipos informáticos en el seno de una inspección tributaria (sentencias de 30 de septiembre de 2010[14], de 23 de abril de 2009 y de 25 de junio de 2009). Estas sentencias, dictadas por la Sala de lo contencioso-administrativo del Tribunal Supremo declararon nulas las pruebas obtenidas por las autoridades fiscales españolas del registro de ordenadores de una

13 STS 11-06-2004- Rec. 471/2003. https://www.poderjudicial.es/search/AN/openDocument/24ca3b7d55fd3805/20040821

14 Véase por todas la STS (Contencioso) de 30-09-2010. Rec. 369/2007 ROJ: STS 5268/2010 -ECLI:ES:TS:2010:5268

empresa por no haber obtenido autorización judicial previa para la entrada en las instalaciones de la empresa en el marco de una inspección tributaria, considerada como "domicilio" a estos efectos y por ello protegida por el derecho fundamental de la inviolabilidad[15].

3.- DERECHO AL SECRETO DE LAS COMUNICACIONES (ART. 18.3 CE)

El artículo 18. 3 CE establece que: "se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial."

La vulneración del derecho fundamental al secreto de las comunicaciones ha sido una de las materias más enjuiciadas por los tribunales españoles en casos de ciberseguridad. En este sentido, hemos recuperado 44 resoluciones del Tribunal Supremo que aplican o se refieren al artículo 18.3 CE bien en exclusiva, bien en conjunción con el artículo 18.1 sobre el derecho a la intimidad.

Como cuestión previa al análisis hemos tenido que diferenciar las resoluciones en las que la interceptación de la comunicación se realizó lícitamente, por parte de las Fuerzas y Cuerpos de Seguridad del Estado y previa autorización judicial, de aquellos casos en los que la interceptación se realizó de forma ilícita, vulnerando el secreto de la comunicación.

A.- Interceptaciones lícitas:

Hemos observado cómo 40 de las 45 sentencias que tratan el tema, lo hacen en virtud de la solicitud de los investigados / condenados, que alegan una vulneración del secreto de sus comunicaciones[16] en

15 Téngase en cuenta que estas sentencias fueron dictadas en el orden contencioso-administrativo y son anteriores al año 2015. En dicho año se introdujo una reforma en la Ley de Enjuiciamiento Criminal española para dotar de un régimen específico a la incautación y registro de equipos informáticos de almacenamiento masivo en el marco de investigaciones policiales. Este régimen es más garantista que el previsto para la entrada y registro en domicilio, que es el supuesto sobre el que versan estas sentencias en aplicación del artículo 18.2 de la Constitución Española.

16 En estos casos también surge la cuestión del tratamiento de datos personales en el marco de investigaciones policiales. Explicamos el tratamiento que los tribunales han dado a este tema en el apartado siguiente.

casos de interceptaciones llevadas a cabo por las Fuerzas y Cuerpos de Seguridad del Estado y que cuentan con la preceptiva autorización judicial. En su gran mayoría, lo hacen enjuiciando delitos sobre tráfico de drogas en los que los cuerpos de policía han interceptado los dispositivos móviles de los sospechosos, en los cuales los tribunales se han limitado a enumerar y explicar los tres requisitos para que una interceptación de comunicaciones se considere licita:

1. La autorización judicial de la medida (que la interceptación de las comunicaciones, así como las prórrogas de las mismas que se consideren necesarias) se autorice previamente por un juez.
2. La proporcionalidad de la medida (que la interceptación se realice solamente por el tiempo y las personas que se haya estimado necesario) fijándose por defecto un periodo de tres meses (art. 579.3º Ley de Enjuiciamiento Criminal) sin perjuicio de las prórrogas que se acuerden, en su caso.
3. La excepcionalidad de la medida (que no exista en Derecho otra medida de eficacia similar y menos gravosa para los derechos fundamentales).

Además de lo anterior, los tribunales han aplicado la doctrina del Tribunal Europeo de Derechos Humanos en esta materia (casos Lüdi, de 5 de junio de 1997 o Kless, de 6 de septiembre de 1998) en los que se exige a las autoridades policiales disponer de "buenas razones" o "fuertes presunciones" a la hora de solicitar a la autoridad judicial la medida de interceptación del secreto de las comunicaciones. Las sentencias de 30 de octubre de 2018[17] o de 4 de junio de 2014[18], ambas de la Sala de lo Penal, son ejemplos de ello.

Cumplidos esos requisitos se puede considerar que la interceptación cumple todas las garantías legales.

17 STS 30-10-2018. Rec. 10736/2017 https://www.poderjudicial.es/search/AN/openDocument/2aa483744def8b15/20181219

18 STS 04-06-2014. Rec. 2058/2013. https://www.poderjudicial.es/search/AN/openDocument/5a3536565ee47c3b/20140624

B.- Concepto de "comunicación" protegida por el secreto:

Los tribunales españoles han elaborado una interesante doctrina jurisprudencial sobre el concepto de comunicación. La comunicación se configura como algo presente, que sucede en el momento, por lo que la incautación de dispositivos (móviles, ordenadores) con conversaciones que ya han tenido lugar (por ejemplo, mensajes de correo electrónico o chat) caen fuera del concepto de "comunicación" y no están amparadas por el derecho al secreto de las comunicaciones, a pesar de que, no obstante, puedan estar protegidas por otros derechos fundamentales, como la intimidad o la protección de datos de carácter personal. En este sentido se pronuncia la sentencia del Tribunal Supremo (Penal) de 13 de febrero de 2014[19] cuando establece que "finalizada la comunicación, el contenido de lo comunicado y los datos asociados quedan fuera del ámbito de protección del art. 18.3 de la Constitución Española"

Por otra parte, la localización de una dirección IP para iniciar unas investigaciones penales tampoco se considera vulneración del secreto de las comunicaciones, como establece la sentencia de 14 de julio de 2010[20] de la Sala de lo Penal del Tribunal Supremo. En la misma línea, pero referida a los códigos IMSI, las sentencias de 13 de febrero de 2013[21], de 18 de junio de 2009[22] y de 18 de diciembre de 2008[23], también de la Sala de lo Penal del Supremo.

19 STS 13-02-2014. Rec. 1729/2013 https://www.poderjudicial.es/search/AN/openDocument/d56f403a5999f414/20140303

20 STS 14-07-2010. Rec. 2476/2009. https://www.poderjudicial.es/search/AN/openDocument/5c73c79a1e1e7c2f/20100812

21 STS 13-02-2013. Rec.644/2012. https://www.poderjudicial.es/search/AN/openDocument/136bca8565f4c3fa/20130222

22 STS 18-06-2009. Rec. 11292/2008 https://www.poderjudicial.es/search/AN/openDocument/56ff90e98c1abada/20090716

23 STS 18-12-2008. Rec. 10542/2008 https://www.poderjudicial.es/search/AN/openDocument/b04369e9ce94a82c/20090129

C.- Diferenciación entre interceptación de comunicaciones y volcado de datos:

Sin perjuicio de que lo señalaremos más adelante en relación con la incautación de dispositivos de almacenamiento masivo en el curso de investigaciones policiales, los tribunales españoles se han planteado si el volcado de datos telemáticos previamente interceptados supone una vulneración del secreto de las comunicaciones. En este sentido, destacamos el Auto del Tribunal Supremo (Penal) de 4 de junio de 2020 que estableció que, si bien el derecho al secreto no se vulnera en los casos de volcado de datos telefónicos previamente interceptados a sospechosos de delitos, sí podría verse vulnerado el derecho a la intimidad del artículo 18.1 de la CE. No obstante, cuando se cumple el requisito de la autorización judicial, el derecho a la intimidad tampoco habrá sido objeto de vulneración.

En casos de urgencia, tal y como se establece en la sentencia del Tribunal Supremo (Penal) de 10 de marzo de 2016[24], puede admitirse el examen de los dispositivos sin consentimiento de los propietarios de los dispositivos e incluso sin previa autorización judicial.

D.- Interceptaciones ilícitas:

De las sentencias analizadas, se han observado cuatro casos de interceptaciones no lícitas de las comunicaciones electrónicas, casi siempre circunscritas al ámbito de las relaciones laborales. Son ejemplos de este tipo de vulneraciones del secreto de las comunicaciones, las sentencias del Tribunal Supremo, (Social), de 24 de septiembre de 2019, que consideró desproporcionado y atentatorio contra el derecho al secreto de las comunicaciones la revisión de todos los correos electrónicos, incluidos los de carácter personal de una trabajadora despedida en el ámbito de una revisión de su ordenador; o la de 23 de octubre de 2018, que presupone una cierta expectativa del trabajador sobre la privacidad de los datos contenidos en su ordenador, por lo que no todas las revisiones del mismo por parte de la empresa serán lícitas; o la de 17 de marzo de 2017, que

24 STS 10-03-2016. Rec. 10633/2015. https://www.poderjudicial.es/search/AN/openDocument/00d9a232d18bfdb8/20160330

establece el alcance del poder de control del empresario sobre los medios informáticos de la empresa, quien deberá establecer con anterioridad las prohibiciones absolutas o relativas de la utilización y control de estos dispositivos. En el epígrafe sobre aspectos laborales de la ciberseguridad, se ofrece una explicación más detallada de estas cuatro resoluciones.

Por su parte, en el ámbito penal, encontramos la sentencia de la Sala Segunda del TS de 29 de mayo de 2012 que declara la nulidad de la interceptación de las comunicaciones por falta absoluta de motivación en la resolución judicial que autorizó la misma.

4.- DERECHO A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y A LA AUTODETERMINACIÓN INFORMÁTICA (HABEAS DATA) [ART. 18.4 CE]

Con los parámetros de búsqueda utilizados, hemos recuperado catorce sentencias que tratan la protección de datos de carácter personal y la autodeterminación informática *(habeas data*) de las que destacamos las siguientes:

A.- Protección de datos personales en casos de descubrimiento y revelación de secretos:

La sentencia del Tribunal Supremo (Penal), de 28 de junio de 2018[25] en un caso de acceso indebido a bases de datos de tráfico para obtener datos de determinadas personas y sus vehículos, calificó dicha conducta como un delito de descubrimiento y revelación de secretos, discutiéndose si la existencia de un perjuicio para el afectado era un elemento necesario para la comisión del delito. Dicha sentencia, considera que es difícil conocer cuándo se produce ese "perjuicio" considerando que no todos los datos están protegidos por el artículo 18 de la Constitución, sino "solamente aquellos de los que se puede predicar una sensibilidad por su pertenencia al ámbito de la intimidad más estricta" con lo que enlaza el derecho a la protección de datos del artículo 18.4 con el derecho a la intimidad

25 STS 28-06-2018. Rec. 2266/2017 https://www.poderjudicial.es/search/AN/openDocument/b45b92bd9bd3f33e/20180919

del artículo 18.1. En esta misma sentencia se declara que el mero acceso a los datos exige que el perjuicio deba ser acreditado, a no ser que estemos hablando de datos sensibles (relativos a la salud, ideología, vida sexual o creencias) en cuyo caso esa exigencia de la acreditación perjuicio no será necesaria. En similares términos, la sentencia del Tribunal Supremo (Penal), de 30 de diciembre de 2009[26], enjuicia si el acceso a una base de datos clínica, al objeto de conocer el nombre de un médico, es una vulneración de la protección de datos además de ser un delito de descubrimiento de secretos. En este caso concreto, el Tribunal Supremo estableció una distinción entre los datos protegidos por la normativa de protección de datos y el precepto constitucional, concluyendo que la identidad (el nombre y los apellidos) de un facultativo, consultados en una base de datos de un hospital por quien ejerce el puesto de coordinador médico, no es predicable de una infracción de protección de datos ni mucho menos de un delito de descubrimiento y revelación de secretos, toda vez que esos datos no pueden tener carácter reservado, ya que incluso aparecen en los listados de los centros de salud o en la tarjeta sanitaria. En este sentido, no puede considerarse que el nombre de un facultativo es un dato que merezca la misma protección, dentro de una historia clínica, que otros datos como los de una patología, sobre todo si es de carácter psíquico.

B.- Protección de datos personales en el curso de investigaciones policiales:

La sentencia del Tribunal Supremo (Penal), de 8 de junio de 2016[27], resolviendo un caso de delito contra la salud pública relacionado con delitos de blanqueo de capitales e integración en organización criminal, llevó a cabo un análisis de la aplicación del art. 18.4 CE en relación con los datos de investigaciones en terrorismo y delincuencia organizada. En estos casos, establece el Tribunal Supremo, que tanto el precepto constitucional como la normativa de protección

26 STS 30-12-2009. Rec. 1142/2009. https://www.poderjudicial.es/search/AN/openDocument/fbae06df82f2a2fb/20100218

27 STS 08-06-2016. Rec. 10545/2015 https://www.poderjudicial.es/search/AN/openDocument/c5395c89637a6169/20160613

de datos española, excluyen el régimen de protección de datos en las formas más graves de persecución del terrorismo y delincuencia organizada.

En el mismo sentido, podemos citar la sentencia del Tribunal Supremo (Penal) de 27 de diciembre de 2010[28], que declara que, si bien el artículo 18.4 de la Constitución establece que "una ley regulará el uso de la informática para proteger y garantizar el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos ciudadanos", dicha "ley" -Ley Orgánica 15/1999, de Protección de Datos de carácter personal, en la actualidad derogada, pero vigente al tiempo de los hechos – otorga una protección que no es aplicable en los casos de investigación de hechos delictivos para encontrar y recabar los datos necesarios para incorporarlos a la investigación, sin necesidad de autorización judicial previa expresa, siempre que dicha actuación sea necesaria y haya resultado proporcionada.

También, la reciente sentencia del Tribunal Supremo (Penal) 2ª, de 15 de junio de 2020[29], en un caso de tráfico de drogas, trata el tema de la interceptación de las comunicaciones por parte de las Fuerzas y Cuerpos de Seguridad del Estado, así como la cesión de datos de comunicaciones electrónicas, que debe ser ajustada al principio de proporcionalidad.

Finalmente, en referencia a la protección de los datos fiscales, la sentencia del Tribunal Supremo (Penal) de 5 de diciembre de 2012[30], se refiere a la aplicación del art. 18.4 CE a los datos fiscales. Esta sentencia declara que la información fiscal de las personas forma parte del derecho a la intimidad, lo que el Tribunal Constitucional de España denomina "intimidad económica": en este sentido, si bien es lícita la solicitud de datos fiscales en el marco de una investigación tributaria, estos deben limitarse a los de concretas operaciones sospechosas, sin que quepa una solicitud de toda la información fiscal de gran cantidad de personas y sociedades.

28 STS 27-12-2010. Rec. 1033/2010. https://www.poderjudicial.es/search/AN/openDocument/d5831e75aea64533/20130116

29 STS 15-06-2020. Rec. 3896/2018 https://www.poderjudicial.es/search/AN/openDocument/7c2aa5b5ead48485/20200707

30 STS 05-12-2012. Rec. 2216/2011. https://www.poderjudicial.es/search/AN/openDocument/d5831e75aea64533/20130116

Para finalizar este apartado, señalamos la sentencia del Tribunal Supremo (Contencioso-Administrativo) de 11 de enero de 2019[31] que confronta los límites del derecho constitucional a la protección de datos y a la libertad informática del artículo 18.4 de la CE con el derecho a la libertad de expresión e información, recogido en el artículo 20 del texto constitucional y también con la categoría de derecho fundamental, en un caso de "derecho al olvido" en el que la Agencia Española de Protección de Datos sancionó a la compañía Google porque el motor de búsqueda desestimó la solicitud formulada por un particular que solicitaba el borrado del buscador de una información particularmente lesiva por injuriosa contra su persona. En esta sentencia, el Tribunal Supremo falló a favor de la Agencia Española de Protección de datos – y, en última instancia, a favor del particular para ejercer su derecho al olvido -, pero porque la noticia alojada en el buscador y cuya eliminación se pretendía no respondía a la veracidad de los hechos.

C.- Doctrina del Tribunal Constitucional sobre el artículo 18.4 CE en relación con la ciberseguridad:

El Tribunal Constitucional, por su parte, ha recogido en las siguientes sentencias, la interpretación del artículo 18.4 CE relativo a la protección de datos, en casos en los que existían cuestiones de ciberseguridad en juego:

En primer lugar, la sentencia de 11 de febrero de 2013[32], resolviendo un recurso de amparo por vulneración del derecho a la protección de datos en un supuesto de grabación de imágenes por cámaras de vídeo vigilancia. Para el Tribunal Constitucional está "fuera de toda duda" que las imágenes grabadas en soporte físico constituyen datos de carácter personal, susceptibles de protección tanto por la Constitución como por la normativa específica de protección de datos, por lo que el responsable del tratamiento debe asegurarse que dichas cámaras no contravengan el derecho fundamental a la

31 STS 11-01-2019. Rec. 5579/2017. https://www.poderjudicial.es/search/AN/openDocument/fa83b4172cfcce71/20190118

32 STC 11-02-2013. Rec. 10522/2009. https://hj.tribunalconstitucional.es/es/Resolucion/Show/23284

protección de datos para lo cual debe informarse de los motivos por los que se recaban las imágenes y más si es para control laboral. En esta sentencia, el Tribunal Constitucional define en qué consiste el derecho fundamental a la protección de datos, el cual "persigue garantizar a la persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado, pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin". En la sentencia del Tribunal Constitucional de 31 de enero de 2013[33], se identifica el derecho fundamental del artículo 18.4 CE con la "libertad informática" definida como "el derecho a controlar el uso de los datos insertos en un programa informático (*habeas data)* y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención". Esta sentencia añade que "la recogida y posterior tratamiento de los datos de carácter personal se ha de fundamentar en el consentimiento de su titular, facultad que sólo cabe limitar en atención a derechos y bienes de relevancia constitucional, de modo que esa limitación esté justificada, sea proporcionada y, además, se establezca por Ley".

5.- COMPETENCIAS EXCLUSIVAS DEL ESTADO EN MATERIA DE SEGURIDAD PÚBLICA (ART. 149.1.29 CE).

Como es sabido, la organización política y territorial española se configura como un Estado descentralizado, dividido en Comunidades Autónomas, estableciéndose una distribución de competencias entre el gobierno central y los gobiernos autonómicos. Para lo que es de interés en el siguiente artículo, se llegó a cuestionar si la ciberseguridad formaba parte de las competencias del gobierno central o si, por el contrario, las comunidades autónomas podían ejercer competencias en materia de seguridad informática y además emitir legislación al respecto, o incluso podría llegarse a una tercera opción, siendo la

33 STC 31-01-2013. Rec. 1024/2004 https://hj.tribunalconstitucional.es/es/Resolucion/Show/23272#complete_resolucion

ciberseguridad una competencia compartida entre administración central y administraciones autonómicas.

Respecto a esta cuestión se pronunció el Tribunal Constitucional en su sentencia de 20 de diciembre de 2018[34], que dirimió un conflicto entre la Administración General del Estado y la Generalidad de Cataluña a cuenta de la creación por parte de esta última, de una "Agencia Catalana de Ciberseguridad".

La Constitución Española establece en su artículo 149 la lista de competencias que caen dentro de la esfera exclusiva del gobierno central, entre las que se incluye la "seguridad pública", sin perjuicio de que las comunidades autónomas puedan crear sus propios cuerpos de policía y en aplicación de este artículo constitucional, el Tribunal Constitucional español declara en esta sentencia que "la ciberseguridad, como sinónimo de la seguridad en la red, es una actividad que se integra en la seguridad pública, así como en las telecomunicaciones", así como que la ciberseguridad forma parte del concepto más amplio de "seguridad nacional", encomendada a organismos de la Administración General del Estado como el Centro Nacional de Inteligencia o el Consejo de Seguridad Nacional, encargado de definir la "estrategia nacional de ciberseguridad, definida en esta sentencia como "el documento estratégico que sirve de fundamento al Gobierno de España para desarrollar las previsiones de la estrategia de seguridad nacional en materia de protección del ciberespacio con el fin de implantar de forma coherente y estructurada acciones de prevención, defensa, detección, respuesta y recuperación frente a las ciberamenazas".

No obstante lo anterior, el Tribunal Constitucional no declaró la inconstitucionalidad de todos los artículos de la ley catalana de ciberseguridad ya que declara la competencia de la comunidad autónoma "en relación con la protección de sus sistemas de información y comunicación", así como para las labores de "autoprotección de los servicios de su administración y de su sector público, para lo que ha de ejercer las funciones de análisis, investigación y respuesta necesarios para restablecer sus propios servicios y garantizar su seguridad."

34 STC 20-12-2018. Rec. 5284/2017 https://hj.tribunalconstitucional.es/es/Resolucion/Show/25831#ficha-tecnica

Como conclusión a este apartado, podemos decir que, si bien la ciberseguridad concebida como una competencia de seguridad pública es una competencia estatal, determinados aspectos de seguridad informática pueden ser desarrollados por las comunidades autónomas en el marco de la protección de sus propios sistemas informáticos.

IV.- JURISPRUDENCIA PENAL EN MATERIA DE PRIVACIDAD Y SEGURIDAD INFORMÁTICA

Dedicamos el siguiente apartado al examen de las sentencias que se han recuperado en nuestro trabajo sobre aspectos penales de ciberseguridad. Hemos identificado sentencias sobre descubrimiento y revelación de secretos, acoso informático a menores, estafas informáticas, blanqueo de capitales por imprudencia o falsificaciones de tarjetas de crédito, del modo que se relacionan a continuación.

IV.1.- DELITOS DE DESCUBRIMIENTO Y REVELACIÓN DE SECRETOS (ARTS. 197, 197 BIS, 197 TER, 197 QUATER, 195 QUINQUES Y 198 CÓDIGO PENAL)

El Código Penal (en adelante, CP) regula el delito de descubrimiento y revelación de secretos. Este delito se tipifica en un capítulo específico para este tipo de conducta, como un tipo de delito contra la intimidad, la propia imagen y la inviolabilidad del domicilio.

A los efectos que interesan a la ciberseguridad, el delito de descubrimiento y revelación de secretos contempla las siguientes conductas referidas al descubrimiento de confidencias:

- Apoderamiento de mensajes de correo electrónico.
- Interceptación de las comunicaciones.
- Utilización de artefactos técnicos de escucha, transmisión, grabación o reproducción del sonido o la imagen.

Además de lo anterior, las penas serán más altas cuando se proceda a la cesión a terceros de los datos secretos descubiertos (revelación).

El CP también tipifica la conducta del acceso ilegítimo a bases de datos y en concreto, castiga el apoderamiento, utilización o modificación *en perjuicio de tercero*, de datos de carácter personal o familiar, que consten en ficheros o registros telemáticos, bien sean éstos de titularidad pública o privada realizado por persona no autorizada a ello.

En otros apartados del artículo, se castigan con penas superiores, los accesos ilegítimos llevados a cabo por los responsables o encargados del fichero de datos, así como la utilización no autorizada de datos personales de la víctima. Asimismo, cuando los datos así descubiertos se cedan a terceras personas (revelación).

El artículo también tipifica en otros apartados como agravantes, el ánimo de lucro, el descubrimiento y la revelación de datos especialmente protegidos (relativos a la salud, orientación sexual, creencias religiosas o políticas), así como la especial protección a menores de edad, o personas necesitadas de especial protección, o cuando el autor sea cónyuge de la víctima, o persona que conviva en análoga relación de afectividad con la misma.

Finalmente, también se tipifica la difusión de imágenes o grabaciones audiovisuales que fueron tomadas en la intimidad del domicilio, u otro lugar fuera del alcance de la mirada de terceros, cuando dichas imágenes puedan menoscabar gravemente la intimidad personal de la persona grabada.

El Código Penal también castiga especialmente cuando las conductas relacionadas en los apartados anteriores son cometidas por quien ostenta la condición de autoridad o funcionario público.

A.- Número de sentencias localizadas en relación con esta conducta:

Nuestro Tribunal Supremo ha tenido ocasión de pronunciarse sobre este tipo de delitos en veintidós ocasiones, según nuestros datos y en nueve de ellas, directamente relacionado con la vulneración de los derechos fundamentales a la intimidad y a la protección de datos y

libertad informática, recogidos en la Constitución Española y de los que nos hemos ocupado en el apartado anterior. Como es lógico, por la propia tipificación del delito, los bienes jurídicos protegidos en todos los casos son la protección de datos de carácter personal y la protección de la intimidad, que están presentes en todas las sentencias, bien por separado o bien ambos en la misma resolución.

B.- Bien jurídico protegido:

En primer lugar, debemos aclarar qué es lo que el Derecho penal protege con esta regulación, lo que se conoce como "bien jurídico protegido" que en los delitos de descubrimiento y revelación de secretos es la libertad informática, pronunciándose en tal sentido la sentencia del Tribunal Supremo español (Penal) de 18 de octubre de 2012[35], que establece que "[l]o que se protege a través de las conductas previstas en el apartado segundo del artículo 197 del Código Penal, es "la libertad informática entendida como derecho del ciudadano a controlar la información personal y familiar que se encuentra recogida en ficheros de datos, lo que constituye una dimensión positiva de la intimidad que constituye el bien jurídico protegido". En el mismo sentido se pronuncian otras sentencias como la de 17 de junio de 2014[36], que declara que se está protegiendo el derecho de los titulares a mantener sus datos secretos u ocultos. Sin embargo, otras resoluciones del mismo Tribunal Supremo, como las de 21 de marzo de 2007[37] y de 25 de mayo de 2017[38], establecieron que el bien jurídico protegido es la "intimidad de la persona".

35 STS 18-10-2012. Rec. 2343/2011 https://www.poderjudicial.es/search/AN/openDocument/45c3f857d312b32c/20121224

36 STS 17-06-2014. Rec. 136/2014 https://www.poderjudicial.es/search/AN/openDocument/e525c11601ba7c26/20141002

37 STS 21-03-2007- Rec. 2051/2005 https://www.poderjudicial.es/search/AN/openDocument/976d74504d8c6c01/20070412

38 STS 25-05-2017. Rec. 142/2017 https://www.poderjudicial.es/search/AN/openDocument/9814bc436a98d6a5/20170714

C.- Concepto de "perjuicio":

El concepto de "perjuicio" en el descubrimiento y revelación de secretos ha sido objeto de una constante doctrina del Tribunal Supremo, dando muestras del interés que esta cuestión suscita. En este sentido puede afirmarse que la doctrina general es que el perjuicio ya se supone con el mero acceso no autorizado a los datos. Como ejemplo de esta doctrina podemos citar la sentencia del Tribunal Supremo (Penal) de 17 de junio de 2014[39], que ya establece que el perjuicio ya existe desde que el autor pone al descubierto los datos que hasta entonces permanecían reservados ya que con esta acción se provoca un daño a sus titulares a mantener sus datos secretos u ocultos. Esta línea argumental ha sido mantenida por otras sentencias posteriores, como la de 25 de mayo de 2017[40] en la que el Tribunal Supremo declara que "ya el mero descubrimiento constituye un perjuicio", o la sentencia de 23 de julio de 2018[41], que en relación a este aspecto declara que "el concepto de 'perjuicio de tercero' en el Código Penal español es muy amplio, de hecho, no requiere que exista perjuicio económico, ni siquiera ánimo de perjudicar".

Siendo esta la doctrina mayoritaria, no han faltado algunas sentencias que se han apartado de este concepto tan amplio del perjuicio, al entender que los datos descubiertos carecían del requisito de pertenencia al ámbito personal o familiar, lo que se refuerza cuando dichos datos pueden ser consultados en bases de datos accesibles al público, como por ejemplo la titularidad de un vehículo privado. En este sentido se pronuncian la sentencia del Tribunal Supremo (Militar) de 24 de septiembre de 2019[42], o la sentencia del Tribunal Supremo (Penal) de 28 de junio de 2018[43].

39 STS 17-06-2014. Rec. 136/2014 https://www.poderjudicial.es/search/AN/openDocument/e525c11601ba7c26/20141002

40 STS 25-065-2017. Rec. 142/2017 https://www.poderjudicial.es/search/AN/openDocument/9814bc436a98d6a5/20170714

41 STS 23-07-2018. Rec. 1909/2017 https://www.poderjudicial.es/search/AN/openDocument/a0b52f86d6f4c196/20180801

42 STS 24-09-2019. Rec. 11/2019.

43 STS 28-06-2018. Rec. 2266/2017. https://www.poderjudicial.es/search/AN/openDocument/b45b92bd9bd3f33e/20180919

D.- Comisión por funcionario público:

Las sentencias analizadas nos muestran que no son infrecuentes los supuestos en los que el delito ha sido cometido por un funcionario público, mediante el acceso a bases de datos públicas: algunos ejemplos de esto son las sentencias del Tribunal Supremo (Penal) de 25 de mayo de 2017[44], en el que se enjuició un caso de acceso a la base de datos de la AEAT para fines distintos de los autorizados; la sentencia de 23 de julio de 2018[45], relativa al acceso por una funcionaria de determinados datos sobre la Seguridad Social de una persona, que además envió a un medio de comunicación; la sentencia de 2 de marzo de 2016[46], relativo al acceso no autorizado por un funcionario a la base de datos del DNI para confeccionar documentos de identidad falsos, las de 3 de febrero de 2016[47] y de 23 de septiembre de 2015[48] – acceso por médicos del sistema público de salud, empleados públicos según el sistema español - a historiales clínicos o la sentencia de 6 de octubre de 2015[49], en la que se ventila el caso de un delito cometido por un juez al consultar y un oficial del juzgado los datos de una persona contenidos en el Registro central de penados y rebeldes. En este sentido, es interesante el razonamiento del Tribunal Supremo, en esta última sentencia citada, cuando declara que el delito informático puede ser cometido por "cualquier persona no autorizada o autorizada fuera de su legítimo ámbito funcional", es decir, aunque el funcionario esté autorizado para la consulta de datos reservados, esto en ningún caso ampara una consulta fuera del estricto cumplimiento de sus funciones.

44 STS 25-05-2017. Rec. 142/2017 https://www.poderjudicial.es/search/AN/openDocument/9814bc436a98d6a5/20170714

45 STS 23-07-2018. Rec. 1909/2017 https://www.poderjudicial.es/search/AN/openDocument/a0b52f86d6f4c196/20180801

46 STS 02-03-2016. Rec. 1055/2015 https://www.poderjudicial.es/search/AN/openDocument/f9315d37f8a28335/20160315

47 STS 03-02-2016. Rec. 943/2015 https://www.poderjudicial.es/search/AN/openDocument/1dc6bf73addecf1c/20160209

48 STS 23-09-2015. Rec. 648/2015 https://www.poderjudicial.es/search/AN/openDocument/7d803377720842c0/20151001

49 STS 06-10-2015. Rec. 456/2015 https://www.poderjudicial.es/search/AN/openDocument/5738cc59381c2223/20151009

E.- Relación con otras conductas:

Aunque lo más normal es que el delito de descubrimiento y revelación de secretos sea enjuiciado como un ataque a la libertad informática (*habeas data*) del artículo 18.4 de la Constitución Española, en algunas ocasiones se ha enjuiciado conjuntamente con otro tipo de conductas atentatorias de la seguridad informática, como el ciberacoso a menores de edad. Son ejemplo de este tipo de casos las sentencias del Tribunal Supremo (Penal) de 27 de junio de 2019[50] o la de 2 de julio de 2015[51]. En estos casos, las víctimas fueron menores de edad a quienes se espió utilizando medios informáticos llegando a menoscabar gravemente su intimidad por medio del acoso de tipo sexual, conducta tipificada en el artículo 183 CP como un supuesto de abuso a menores. La STS de 20 de julio de 2020[52] (Penal) resuelve sobre un acceso no autorizado a los mensajes de móvil por la pareja de la víctima, y en la de 21 de junio de 2016[53] (Penal) el Tribunal Supremo condena a un individuo por el delito de acceso no autorizado al WhatsApp y al teléfono móvil de la víctima. También incluimos en este apartado la sentencia (Penal) de 9 de enero de 2019[54], por la que se enjuicia por un delito de descubrimiento y revelación de secretos con el agravante de que los datos estaban referidos a la vida sexual de la víctima.

F.- Instalación de componentes:

Sobre instalación de componentes o artefactos cuando son instalados en el propio equipo informático –como puede ser un software de medición del tráfico de Internet–, la jurisprudencia española establece que, si bien ello no está prohibido, sí lo estará cuando, a resultas de

50 STS 27-06-2019. Rec. 10732/2018. https://www.poderjudicial.es/search/AN/openDocument/816b5890ad53572f/20190708

51 STS 02-07-2015. Rec.2153/2014. https://www.poderjudicial.es/search/AN/openDocument/09452aec18cd3aa7/20150728

52 STS 20-07-2020. Rec. 3736/2018 https://www.poderjudicial.es/search/AN/openDocument/e281f40ceee77df2/20200811

53 STS 21-06-2016. Rec. 10139/2016 https://www.poderjudicial.es/search/AN/openDocument/12887d373edd7cf6/20160704

54 STS 09-01-2019. Rec. 10336/2018 https://www.poderjudicial.es/search/AN/openDocument/6eb086a1aedb9bf6/20190205

la instalación del programa, se descubren datos protegidos por la libertad informática o el derecho a la intimidad. En este sentido se expresa la sentencia del Tribunal Supremo (Penal) de 21 de marzo de 2007[55], que como resultado del volcado de datos que hizo el programa, el acusado descubrió páginas web que demostraban la infidelidad de la esposa y que posteriormente utilizó en el juicio de divorcio, por lo que fue condenado por un delito de descubrimiento y revelación de secretos.

G.- Nivel de seguridad del sistema informático:

A los efectos de la jurisprudencia española es indiferente el mayor o menor grado de protección de los sistemas informáticos para la comisión del delito de descubrimiento y revelación de secretos, siendo lo relevante a efectos penales el acceso no autorizado y el que los datos incluidos en el sistema tengan carácter reservado, como establece la sentencia del Tribunal Supremo (Penal) de 17 de enero de 2013[56].

IV. 2.- CIBERACOSO CONTRA MENORES DE 16 AÑOS (ART. 183 CP)

Seis sentencias del Tribunal Supremo han sido recuperadas en nuestro análisis, las cuales han resuelto asuntos de seguridad informática en los que han aparecido como víctimas menores de dieciséis años.

El Código Penal español regula en su artículo 183 los delitos de abusos sexuales a menores y en su artículo 183 *ter,* sanciona a quienes utilizan Internet o medios informáticos o telemáticos para contactar con menores de dieciséis años con estos fines. En terminología anglosajona, estos delitos se califican como "*child grooming*", expresión que ha utilizado también el Tribunal Supremo español.

55 STS 21-03-2007. Rec. 2051/2015 https://www.poderjudicial.es/search/AN/openDocument/976d74504d8c6c01/20070412

56 STS 17-01-2013. Rec. 903/2012 https://www.poderjudicial.es/search/AN/openDocument/799b666d1d7dd06b/20130204

Destacamos en este apartado, la sentencia del Tribunal Supremo (Penal) de 10 de diciembre de 2015[57] en el que se acosaba a una menor de dieciséis años por webcam y la red social Facebook. En este caso se discutió la validez de la prueba obtenida por la madre al entrar en la cuenta de Facebook de su hija menor de edad por si en este caso la madre podía haber vulnerado el derecho fundamental a la intimidad de la hija. En este caso, el Tribunal Supremo valora las circunstancias del caso, prevaleciendo la patria potestad de la madre frente al derecho a la intimidad de la menor por sus datos de Facebook, además de que la menor no niega el haber dado permiso a su madre para el acceso a su cuenta y máxime que el acceso sirvió para la persecución de un delito.

Un supuesto similar se enjuicia en la sentencia de 4 de diciembre de 2015, en la que el Tribunal Supremo (Penal) declaró que el que un progenitor facilite a la policía las claves de acceso del ordenador del menor que estaba siendo víctima de ciberacoso no vulnera el secreto de las comunicaciones del artículo 18.3 de la CE. En cuanto a los requisitos de autorización judicial para el visionado de los archivos, esta sentencia destaca que en determinados supuestos bastaría con que el juez emita un Auto en lugar de una providencia, cuyos requisitos formales son mayores.

Finalmente, y para concluir este epígrafe, destacamos la sentencia de 24 de febrero de 2015[58], del Tribunal Supremo e (Penal) que establece la definición de *child grooming* como acoso informático a menores. Esta sentencia define el acoso informático menores como "las acciones realizadas deliberadamente con el fin de establecer una relación y un control emocional sobre un menor con el fin de preparar el terreno para el abuso sexual del menor", aclarando además que "[e]l contacto tiene que ser por medio tecnológico. La Ley se refiere a Internet, teléfono o cualquier otra tecnología de la información y la comunicación", el listado es abierto para cubrir cualquier tecnología de comunicación presente o que surja en el futuro.

57 STS 10-12–2015. Rec. 912/2015. https://www.poderjudicial.es/search/AN/openDocument/910ca00c9b21791c/20160219

58 STS 24-02-2015. Rec. 1774/2014. https://www.poderjudicial.es/search/AN/openDocument/12a65a0eae7bcce0/20150323

IV.3.- ESTAFA INFORMÁTICA CON POSIBLE AGRAVANTE (ARTS. 248.1 Y 2 Y 250.6º CP)

El Código Penal define la estafa informática como la conducta cometida por "los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro. Además, existe una variante agravada de este delito en los casos en los que el delito se cometa "con abuso de las relaciones personales existentes entre víctima y defraudador, o aproveche éste su credibilidad empresarial o profesional".

La estafa informática en Derecho español comprende un tipo muy diverso de supuestos. El Tribunal Supremo ha considerado como delito de estafa informática la alteración por funcionario público de la base de datos de gratificaciones extraordinarias (bonus) para hacer beneficiario a su cónyuge, sentencia del Tribunal Supremo (Penal) de 6 de noviembre de 2007[59]. Esta sentencia define la estafa informática como "toda actividad fraudulenta valiéndose de medios informáticos". El Tribunal Supremo aclara, no obstante, que el autor material del fraude informático puede ser persona distinta del responsable del fichero.

Otro supuesto de estafa informática enjuiciado por el Tribunal Supremo fue el de una empleada de una oficina bancaria que, prevaliéndose de su puesto, alteró el sistema informático para desviar fondos a su cuenta bancaria y las de familiares y amigos.

Entre las conductas de la estafa informática se encuentra el *phishing* o conductas de suplantación. El Tribunal Supremo (Penal) tuvo ocasión de enjuiciar un caso de estafa informática por suplantación en su sentencia de 2 de diciembre de 2014[60].

Un agravante de la estafa informática es su comisión por parte de un funcionario público. El artículo 390 CP considera un agravante la alteración de un sistema informático por parte de un funcionario, como se explica en la sentencia de 6 de noviembre de 2007, comentada anteriormente.

59 STS 06-11-2007. Rec. 753/2007. https://www.poderjudicial.es/search/AN/openDocument/35063cb4dbabc9f3/20071122

60 STS 02-12-2014. Rec. 664/2014. https://www.poderjudicial.es/search/AN/openDocument/32aa4ceb2bf7a528/20150206

IV.4.- BLANQUEO DE CAPITALES IMPRUDENTE (ART. 301.3 CP):

El Código Penal castiga con penas de prisión de seis meses a dos años a la persona que "adquiera, posea, utilice, convierta, o transmita bienes, sabiendo que éstos tienen su origen en una actividad delictiva, cometida por él o por cualquiera tercera persona, o realice cualquier otro acto para ocultar o encubrir su origen ilícito". En nuestra investigación hemos comprobado que la Sala de lo Penal del Tribunal Supremo ha tenido ocasión de enjuiciar este tipo de conductas en las sentencias de 3 de noviembre de 2016[61], de 27 de julio de 2015[62] y de 25 de octubre de 2012[63] en relación con delitos de estafa informática por medio de suplantación, en los que se han empleados a personas para depositar temporalmente los fondos sustraídos ilegítimamente por suplantación de páginas web, constituyendo una forma de blanqueo de capitales en el que en los tres casos los implicados desconocían o podían desconocer la procedencia ilícita de los fondos recibidos, los cuales tenían que transferir por medio de empresas de envío de remesas a países del extranjero.

IV. 5.- FALSIFICACIÓN DE TARJETAS DE CRÉDITO (SKIMMING) [ART. 399 BIS CP]

Solamente hemos localizado un caso enjuiciado por el Tribunal Supremo en relación con la falsificación de tarjetas bancarias. No obstante, la sentencia trata de una cuestión de competencia entre tribunales de una u otra población a causa de una presunta estafa de compras masivas de terminales móviles con tarjetas bancarias falsificadas que se venden en Internet a través de una red social.

61 STS 03-11-2016. Rec.469/2016. https://www.poderjudicial.es/search/AN/openDocument/7b5b3847a81ca830/20161111

62 STS 27-07-2015. Rec. 189/2015. https://www.poderjudicial.es/search/AN/openDocument/4fa92e3b0457241b/20150818

63 STS 25-10-2012. Rec. 2422/2011. https://www.poderjudicial.es/search/AN/openDocument/36942f02bd94a852/20121224

V.- JURISPRUDENCIA ESPECÍFICA SOBRE PROTECCIÓN DE DATOS

Los Tribunales Supremo y Constitucional han dictado una serie de sentencias enjuiciando supuestos que relacionan la seguridad informática con la normativa de protección de datos de carácter personal española dictada en desarrollo del artículo 18.4 de la Constitución anteriormente referido. En este sentido, hemos localizado en nuestra investigación que nuestros Altos Tribunales han tenido la ocasión de aplicar determinados preceptos de la normativa de protección de datos vigente en ese momento, Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (derogada en la actualidad por la entrada en vigor del Reglamento Europeo de Protección de Datos y por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los derechos digitales). Los apartados que se enuncian a continuación hacen referencia a la normativa de 1999, vigente al tiempo de enjuiciamiento de los hechos.

V1.- LA VOZ COMO DATO PERSONAL (ART. 2.3. DE LA LO 15/1999):

Según disponen dos sentencias del Tribunal Supremo (Contencioso-Administrativo) dictadas el 22 de junio de 2020[64], las grabaciones de voz se consideran datos de carácter personal, por lo que su tratamiento debe adecuarse a las previsiones de la normativa de protección de datos española. En ambas sentencias se enjuicia la procedencia de unas sanciones de la Agencia Española de Protección de Datos a una empresa cuyo como objeto social son las bromas telefónicas entre particulares. La cuestión jurídica a dirimir es que la empresa está obligada a custodiar las grabaciones telefónicas con todas las garantías de la normativa de protección de datos y sólo cuando el "bromista" quiere compartir la grabación en redes sociales, es cuando la empresa queda libre de tales obligaciones por exceder de su ámbito de actuación.

64 STS 22-06-2020. Rec. 2134/2019 y Rec. 4958/2019. https://www.poderjudicial.es/search/AN/openDocument/13f5b0e40782fc6c/20200707 https://www.poderjudicial.es/search/AN/openDocument/74daad89b000410e/202007074958/2019

V2.- CONSENTIMIENTO DEL AFECTADO (ART. 6 LO 15/1999):

La sentencia del Tribunal Supremo de 2 de febrero de 2017[65] (Social) dirime el alcance del consentimiento del afectado para la utilización de sus datos de carácter personal en el ámbito de las relaciones laborales. En este caso, se enjuiciaba la validez de la utilización de las cámaras de seguridad como prueba del incumplimiento del trabajador de su horario de trabajo para proceder a su despido disciplinario, toda vez que el trabajador no había dado su consentimiento expreso a la captación de su imagen por dichas cámaras. A pesar de que la sentencia cuenta con un voto particular, la mayoría de la Sala de lo Social del Tribunal Supremo, entendió válida la prueba obtenida a través de las grabaciones de las cámaras de seguridad y establece una interesante doctrina respecto a la recogida y tratamiento de imágenes en las relaciones laborales, con base en los siguientes argumentos: (i) que la instalación de las cámaras era pública y conocida por los trabajadores (ii) la ausencia de "elemento sorpresivo" que permita al trabajador argumentar que no sabía que estaba siendo grabado (iii) la propia finalidad de las cámaras de vídeo vigilancia, que en general, es documentar irregularidades en la empresa y (iv) que el consentimiento del afectado en estos casos debe entenderse implícito en el marco de las relaciones laborales.

V.3.- DERECHO AL OLVIDO (ART. 6.4 LO 15/1999):

En nuestra investigación y con los comandos de búsqueda aplicados, hemos localizado una única sentencia del Tribunal Supremo, referida al derecho al olvido, recogido en el artículo 6.4 de la LO 15/1999 (Sentencia del Tribunal Supremo, sala Contencioso-Administrativo, de 11 de enero de 2019[66]) sobre el derecho de un particular a solicitar a Google la retirada de una información injuriosa. El Supremo ponderó en esta sentencia la prevalencia entre el derecho al honor del ofendido y el derecho a la libertad de información del buscador, prevaleciendo

65 STS 02-02.2017. Rec. 554/2016. https://www.poderjudicial.es/search/AN/openDocument/b5f9f44350651dc7/20170313

66 STS 11-01-2019. Rec. 5579/2017. https://www.poderjudicial.es/search/AN/openDocument/fa83b4172cfcce71/20190118

en este caso el primero por ser la información inexacta y no responder a la veracidad de los hechos.

V.4.- DATOS REFERIDOS A LA SALUD COMO "DATOS ESPECIALMENTE PROTEGIDOS" Y SOBRE EL DEBER DE SECRETO (ARTS. 7.3 Y 10 LO 15/1999):

La infracción del deber del titular del fichero de guardar secreto profesional respecto de los datos contenidos en el mismo, regulado en el artículo 10 de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal–norma derogada en la actualidad, pero vigente al tiempo de los hechos-, figura en la sentencia del Tribunal Supremo (Contencioso-Administrativo) de 2 de diciembre de 2011[67], recabada en nuestra investigación, en la que se enjuicia el caso de un juez que consulta indebidamente los registros informáticos para consultar las bajas de los empleados del juzgado. No estamos, según el Supremo, ante un delito de descubrimiento y revelación de secretos, sino ante una infracción administrativa, pero que no puede ser sancionada por la Agencia de Protección de Datos, por ostentar el autor de la infracción la condición de funcionario público, al ser juez en España. Lo interesante de esta sentencia es la determinación del alcance de la potestad sancionadora de la Agencia Española de Protección de Datos, la cual, a criterio del tribunal, alcanza a los sujetos de derecho privado, pero no a los funcionarios públicos, sin perjuicio de la apertura de un expediente disciplinario. Esta sentencia también hace aplicación del artículo 7.3. de la Ley de protección de datos española, que considera como "especialmente protegidos" los datos de carácter personal referidos, en el caso de la sentencia estudiada, a la salud.

V.5.- RECOGIDA Y TRATAMIENTO DE DATOS PARA FINES POLICIALES (ART. 22.2. LO 15/1999):

En el supuesto de la recogida y tratamiento de datos por las Fuerzas y Cuerpos de Seguridad del Estado traemos a colación la sentencia del

67 STS 02-12-2011. Rec. 2706/2008. https://www.poderjudicial.es/search/AN/openDocument/977fd1bc92cb6d8f/20120102

Tribunal Supremo (Penal) de 13 de febrero de 2013[68], que resuelve, precisamente un supuesto de una presunta vulneración del derecho al secreto de las comunicaciones del artículo 18.3 de la Constitución, ya explicado, en el marco de una investigación policial en la que los agentes acceden al código IMSI el cual, constituye, según el Tribunal Supremo, un dato susceptible de protección constitucional en los términos del artículo 18.4 CE, también objeto de estudio en este trabajo. No obstante, el tribunal español aplica en este caso lo dispuesto en el artículo 22.2 de la Ley Orgánica 15/1999, que permite "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". En el caso enjuiciado, el Tribunal Supremo entendió que los códigos IMSI interceptados obedecían a la finalidad descrita en la norma.

i. Principio de seguridad de los datos (art. 9 LO 15/1999) y el deber de mantenimiento de los ficheros con las debidas condiciones de seguridad [art. 44.3 h) LO 15/1999]:

El artículo 44.3, h) de la LO 15/1999, vigente en el momento de comisión de los hechos, tipifica como infracción grave "mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen". En la sentencia del Tribunal Supremo (Contencioso-Administrativo) de 4 de noviembre de 2013[69], se estudia el caso de una sanción de la Agencia Española de Protección de Datos a un colegio profesional, por infracción de lo dispuesto en el artículo 9 de la LOPD, que establece que "el responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a

68 STS 13-02-2013. Rec. 644/2012. https://www.poderjudicial.es/search/AN/openDocument/136bca8565f4c3fa/20130222

69 STS 04-11-2013. Rec. 1293/2011. https://www.poderjudicial.es/search/AN/openDocument/fda8d095e4d31e0e/20131211

que están expuestos, ya provengan de la acción humana o del medio físico o natural". Dicho colegio profesional fue víctima de un ataque informático a causa de las vulnerabilidades del sistema informático, las cuales ya fueron advertidas en una auditoría informática previa. Se confirma en sede judicial la procedencia de la sanción, pese a que el colegio profesional adoptó toda una serie de medidas diligentes una vez que se produjo el ataque.

VI.- ALGUNOS ASPECTOS PROCESALES

VI. 1.- SOBRE LA INCAUTACIÓN DE ELEMENTOS INFORMÁTICOS EN EL CURSO DE INVESTIGACIONES POLICIALES [ART. 588 SEXIES A) CP]

La Ley de Enjuiciamiento Criminal, establece en su artículo 588 *sexies,* -introducido en una reforma del año 2015-, el régimen aplicable a la incautación y registro de dispositivos de almacenamiento masivo de información por parte de las Fuerzas y Cuerpos de Seguridad del Estado. En síntesis, este precepto establece un régimen particular y diferenciado para proceder a la incautación y registro del contenido de dispositivos de almacenamiento masivo de datos, otorgando a la persona investigada mayores garantías en el momento del decomiso, precisándose una autorización judicial previa y expresa al respecto, sin que sea suficiente un permiso judicial de entrada y registro domiciliario.

En nuestro análisis, hemos detectado siete resoluciones que aplican o se refieren a este precepto legal en sentencias del Tribunal Supremo sobre cuestiones de seguridad informática, de las que destacamos en primer lugar, la sentencia del Tribunal Supremo (Penal) de 15 de junio de 2020[70], que, enjuiciando un caso de acoso informático a través del ordenador y la *webcam*, resume la doctrina del Alto Tribunal respecto de las razones por las que se regula un régimen más garantista para el investigado respecto de estos dispositivos, que el ordinario de entrada y registro en domicilio.

70 STS 15-06-2020. Rec. 3777/2018. https://www.poderjudicial.es/search/AN/openDocument/5e4a4ac6693ac240/20200713

(i) "Un ordenador no es una simple pieza de convicción ocupada en un registro".

(ii) "El acceso a la información contenida en un ordenador precisa de una justificación singularizada y distinta de la que se exige para una entrada y registro en domicilio".

(iii) La información contenida en un ordenador normalmente estará afectada por los derechos constitucionales a la intimidad (art. 18.1 CE) y al secreto de las comunicaciones (art. 18.3 CE).

Esta sentencia explica también como la policía puede obtener las claves del ordenador por el propio investigado, si éste las facilita por su propia voluntad en el marco de una investigación:

(i) El acto de facilitar las claves por el propio investigado es una decisión libre y voluntaria, entendida como un acto de colaboración con las Fuerzas y Cuerpos de Seguridad del Estado en el marco de una investigación.

(ii) La entrega de las claves puede hacerse de manera expresa, verbalmente o por escrito o tácita mediante actos que dan lugar inequívocamente a que se están facilitando esas claves a los investigadores. De todo ello debe tomarse acta en las diligencias policiales.

(iii) Si bien no es precisa la asistencia de abogado para este trámite, la sentencia aconseja contar con su presencia por ser muy recomendable y para evitar que en sede judicial se impugne la prueba obtenida a través de las claves voluntariamente facilitadas. Además, debe quedar claro que las claves de ordenador se facilitan por el investigado de forma totalmente libre, sin que le influyan las circunstancias "ambientales" del registro.

También refiriéndose a este artículo, podemos citar la sentencia del Tribunal Supremo (Penal) de 14 de octubre de 2019[71], la cual a su vez cita la doctrina de otra sentencia previa -de 23 de octubre de 2018[72]-, que hablaba del tratamiento jurídico más garantista otorgado

71 STS 14-10-2019. Rec. 1379/2019. https://www.poderjudicial.es/search/AN/openDocument/af32ba6b3debc596/20191018

72 STS 23-10-2018. Rec. 1674/2017. https://www.poderjudicial.es/search/AN/openDocument/bf7752f0b6d21b41/20181120

a los dispositivos de almacenamiento masivo de información, como merecedor de "un plus de diligencia específica frente al registro de otros bienes muebles e inmuebles", en el sentido de que el registro de este tipo de dispositivos puede implicar "desnudar virtualmente a una persona", por lo que conviene "un tratamiento unitario a partir de la proclamación de un derecho del individuo al entorno digital"; entendido como un "derecho de nueva generación como es la autodeterminación informativa".

Finalmente, y a pesar de todo el sistema de garantías articulado en torno a los derechos del investigado frente al comiso y registro de sus dispositivos de almacenamiento de datos, existe una excepción contenida en el epígrafe 4 del artículo 588 *sexies* c) que permite la incautación y acceso a los datos sin autorización judicial en casos de urgencia que hagan absolutamente imprescindible la incautación y el análisis del contenido del dispositivo, comunicándolo a la autoridad judicial en el plazo de máximo de veinticuatro horas, mediante escrito motivando las razones de urgencia, tal y como refiere la sentencia del Tribunal Supremo (Penal) de 23 de enero de 2019[73].

Sobre la incautación y registro de dispositivos en el ámbito de las relaciones laborales, hacemos referencia en el siguiente apartado.

VII.- ASPECTOS LABORALES

Dedicamos las siguientes líneas a comentar brevemente la jurisprudencia en materia laboral que hemos recuperado en el marco de nuestro trabajo. En todos los casos, se han discutido vulneraciones de derechos como la intimidad o el secreto de las comunicaciones, en el ámbito laboral en el que, además, se ha encontrado algún componente de seguridad informática.

73 STS 23-01-2019. Rec. 10495/2017. https://www.poderjudicial.es/search/AN/openDocument/8c4547f6bd300962/20190201

VII.1.- GRABACIONES CON CÁMARAS DE VIGILANCIA EN EL ÁMBITO DE LA EMPRESA:

Sobre el empleo de las grabaciones de cámaras de video vigilancia por la empresa sin consentimiento expreso del trabajador afectado, es obligado retomar el comentario de la sentencia del Tribunal Supremo (Social) de 2 de febrero de 2017 incluido en el epígrafe sobre normativa de protección de datos anterior, en la que se daba por ajustado a derecho el despido del trabajador utilizando como prueba las imágenes de las cámaras de vigilancia de la empresa. Sin embargo, la doctrina del Tribunal Constitucional es radicalmente la contraria, como se desprende de la sentencia de 11 de febrero de 2013 en la que se ponderan el derecho constitucional a la protección de datos y a la autodeterminación informativa del artículo 18.4 CE, con el artículo 54.2 a) del Estatuto de los Trabajadores que permite sancionar con el despido las conductas del trabajador consistentes en el abuso de confianza y la transgresión de la buena fe contractual. En esta sentencia del Tribunal Constitucional de 2013, se declara, sin embargo, que, sin el consentimiento expreso y previo del afectado para que su imagen pueda ser captada con fines de control empresarial, como, en este caso, vigilar el cumplimiento de su jornada de trabajo, la empresa no puede utilizar como prueba para el despido las grabaciones del trabajador que demuestren su incumplimiento de jornada. Estas dos sentencias son buena prueba de lo controvertido del asunto y de las dos posiciones existentes sobre la capacidad empresarial para controlar la actividad laboral y sus límites por posibles afectaciones al derecho a la intimidad de las personas trabajadoras.

VII.2.- SECRETO DE LAS COMUNICACIONES EN EL MARCO DE LAS RELACIONES LABORALES:

En el marco de la protección del secreto de las comunicaciones en la jurisdicción social, hemos recuperado tres resoluciones del Tribunal Supremo (Social) que declararon la vulneración por parte de la empresa de tal derecho fundamental y todo ello enmarcado en un contexto de seguridad informática. En primer lugar, la sentencia

de 24 de abril de 2017[74], declaró que la empresa no podía exigir el conocimiento previo del contenido de las comunicaciones sindicales, como requisito para que los representantes de los trabajadores pudieran acceder a la lista de correo electrónico de los empleados con el fin de enviarles comunicaciones electrónicas, por vulnerar el derecho fundamental al secreto de las comunicaciones establecido en el artículo 18.3 CE. Por su parte, la sentencia (Social) de 17 de marzo de 2017[75], declaró que vulneraba este mismo derecho de una trabajadora de baja por incapacidad temporal, el acceso a su ordenador sin su consentimiento, aunque fuese con el propósito de "poner al día el trabajo atrasado" de la trabajadora, pero que derivó en el "descubrimiento" de correos personales entre la trabajadora y su abogado desvelando la estrategia a seguir en una reclamación de reducción de jornada. Finalmente, el Auto de 24 de enero de 2019,[76] que inadmite el recurso de casación interpuesto tanto por empresa como por la trabajadora, declara que el acceso por la empresa al ordenador y al correo electrónico de la trabajadora posteriormente despedida vulneran el derecho fundamental al secreto de las comunicaciones si a pesar de la existencia de un protocolo empresarial sobre uso del correo electrónico, podía generarse una cierta expectativa de privacidad en su utilización por los trabajadores.

Para concluir este apartado debemos volver a traer a colación la sentencia del Tribunal Supremo (Penal) de 23 de octubre de 2018[77], antes citada, pues, a pesar de ser una resolución dictada por la jurisdicción penal, se enmarca en el ámbito laboral. En esta resolución se establece que el acceso al ordenador de un trabajador debe realizarse con medios poco invasivos como, por ejemplo, programas informáticos de filtrado por palabras clave, no siendo lícito, ni siquiera, que el acceso al ordenador se haga en presencia de notario, ya que, en el caso de que no exista una política clara de uso del ordenador

74 STS (Social) de 24-04-2017. Rec. 245/2016 https://www.poderjudicial.es/search/AN/openDocument/f53dc07956569d7b/20170915

75 STS (Social) de 17-03-2017. Rec. 55/2015. https://www.poderjudicial.es/search/AN/openDocument/a6bfce4b84e467ca/20170411

76 ATS (Social) de 24-09-2019. Rec. 4940/2018. https://www.poderjudicial.es/search/AN/openDocument/b65c2e014c6f6466/20191028

77 STS (Penal) de 23-10-2018. Rec. 1674/2017 https://www.poderjudicial.es/search/AN/openDocument/bf7752f0b6d21b41/20181120

corporativo exclusivamente para fines de trabajo, se crea una "expectativa de confidencialidad" que no puede ser desconocida por el empresario. Ahora bien, esta expectativa tampoco puede convertirse en una suerte de impedimento para que el empleador haga uso de sus facultades de control, especialmente en casos de utilización no consentida del equipamiento informático.

VIII.- CONCLUSIONES Y TRABAJO FUTURO

A continuación se esbozan las principales conclusiones que se han extraído del trabajo realizado:

1. Teniendo en cuenta el largo período de tiempo que se ha analizado (veinticinco años) y la cantidad de sentencias que publican nuestros Altos Tribunales cada año[78], el número de resoluciones judiciales recogidas en la selección, 117, podemos indicar que es muy reducido. Dos consideraciones nos asaltan al respecto:

   Por un lado, la escasa relevancia del asunto abordado desde un punto de vista judicial. Lo cual puede ser, bien porque la materia no tenga la suficiente importancia, bien porque sea novedosa, bien porque los asuntos se resuelven en instancias inferiores. Nos decantamos más por las dos últimas posibilidades frente a la primera, si bien para refrendar nuestra hipótesis sería necesario el análisis de sentencias de juzgados y tribunales inferiores en la jerarquía judicial española en una futura línea de trabajo que se abre tras esta investigación.

78 Para conocer el dato del número total de sentencias publicadas, ver como botón de muestra, CONSEJO GENERAL DEL PODER JUDICIAL, *Memoria del Tribunal Supremo 2019,* 2020*,* accesible en:
https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Tribunal-Supremo/Actividad-del-TS/Memoria-del-TS/Memoria-2019-TRIBUNAL-SUPREMO. En este documento se recoge que en el año 2019 el Tribunal Supremo español dictó en total 4.141 sentencias. La sala primera, de lo Civil, 701 sentencias, (página 57 del documento); la sala segunda, de lo Penal, 653 (página 72); la sala tercera, de lo Contencioso-Administrativo 1.900 sentencias (página 91) y, por su parte, la sala cuarta, de lo Laboral, dictó un total de 887 sentencias (página 117).
También, consúltese, TRIBUNAL CONSTITUCIONAL DE ESPAÑA, *Memoria 2019,* 2020, accesible en: https://www.tribunalconstitucional.es/es/memorias/Paginas/default.aspx. En la memoria 2019 del Tribunal Constitucional se puede conocer que dictó un total de 178 sentencias (dato recogido en la página 43).

Por otro lado, como el número de sentencias es pequeño, el haberlas localizado y hacer accesible el listado de las resoluciones hace que tenga más valor el trabajo llevado a cabo en esta investigación.

2. La ciberseguridad en los tribunales españoles es fundamentalmente una cuestión de carácter penal. En este sentido, observamos que la tendencia es el enjuiciamiento de casos por la Sala de lo Penal del Tribunal Supremo en los que se combina la protección de los derechos fundamentales a la intimidad, a la protección de datos y al secreto de las comunicaciones, con la comisión de delitos informáticos como el acceso indebido a bases de datos, la suplantación, el ciberacoso o las falsificaciones.

   No obstante lo anterior, hemos observado que con nuestros comandos de búsqueda no hemos recuperado ninguna sentencia del Tribunal Supremo referida al artículo 264 del Código Penal, que hace referencia al tipo específico de alteración o borrado de datos en sistemas informáticos.

3. Avanzando en el detalle de los asuntos penales de las sentencias seleccionadas, identificamos los siguientes resultados:

   A. En relación al delito descubrimiento y revelación de secretos:

      1. El concepto de perjuicio debe entenderse de un modo amplio pues, según el Tribunal Supremo español, se supone que existe un perjuicio con el mero acceso no autorizado a los datos, salvo en circunstancias muy excepcionales como es el caso de que los datos se encuentren en bases de datos accesibles al público en general.

      2. El delito puede ser cometido por un funcionario público, aunque esté autorizado para la consulta de datos reservados si su acceso no se realiza en el estricto cumplimiento de sus funciones.

      3. La instalación de componentes informáticos está permitida, salvo que con ellos se consiga una información que luego sea revelada para un uso que no se había permitido de la misma.

4. El nivel de seguridad informática del equipo en el que se conservan los datos que son revelados indebidamente es indiferente para condenar por este delito. Por tanto, lo determinante a efectos penales es el acceso no autorizado y el que los datos incluidos en el sistema tengan carácter reservado.

B. Por lo que respecta al delito de Ciberacoso contra menores, nuestra jurisprudencia ha definido el comportamiento, dejando abierto el listado de medios a través de los cuales se realiza el ilícito, para contemplar cualquier tecnología de comunicación presente o que surja en el futuro. Asimismo, el Tribunal Supremo ha avalado la prevalencia de la patria potestad sobre la intimidad del menor cuando una madre entra en la cuenta de una red social de su hijo y a partir de ahí se investiga la comisión de un delito.

C. En cuanto al delito de estafa informática, resaltar que en él se incluyen diversos comportamientos que incluso han dado lugar a supuestos de blanqueo de capitales. Asimismo, la jurisprudencia ha aplicado el posible agravante por abuso de las relaciones personales existentes entre víctima y defraudador, o que sea ejecutado aprovechando éste su credibilidad empresarial o profesional.

Para terminar con este punto, en relación a la incautación y registro de dispositivos de almacenamiento masivo de información por parte de las Fuerzas y Cuerpos de Seguridad del Estado, se ha establecido un auténtico sistema de garantías articulado en torno a los derechos del investigado frente al comiso y registro de sus dispositivos de almacenamiento para evitar "desnudar virtualmente a una persona", proclamando un "derecho del individuo al entorno digital". En este sentido, el Alto Tribunal español sostiene que el acceso a la información contenida en un ordenador precisa de una justificación singularizada y distinta de la que se exige para una entrada y registro en domicilio.

4. La jurisprudencia ha determinado que la ciberseguridad se integra en el concepto de seguridad pública al englobar la

seguridad en la red y, por tanto, es una competencia del Estado. Ahora bien, determinados aspectos pueden ser desarrollados por las Comunidades Autónomas en el marco de la protección de sus propios sistemas informáticos.

5. En materia de protección de datos, todavía nuestros tribunales Supremo y Constitucional – en la fecha de redacción de estas líneas – no han tenido oportunidad de pronunciarse sobre el alcance del nuevo régimen en esta materia, es decir, el Reglamento Europeo de Protección de Datos y la nueva normativa española al respecto, denominada "Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales".

   En esta temática, el Tribunal Supremo ha tenido que dirimir conflictos que afectan hasta seis asuntos diferentes, a saber: la voz como dato personal; el consentimiento del afectado para el tratamiento de datos; el derecho al olvido (priorizando el del afectado sobre la red social, fundamentalmente por la inexactitud de los datos recogidos); los datos de salud como "especialmente protegidos"; la recogida y tratamiento de datos para fines policiales (en la que se permite el acceso a los códigos IMSI interceptados porque resultan necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales) y, en fin, sobre el principio de seguridad de los datos, esto es, el deber de mantenimiento de los ficheros con las debidas condiciones de seguridad (validando una sanción de la autoridad administrativa española en la materia porque ya se había avisado a la institución infractora sobre la vulnerabilidad de su sistema informático).

   Algunas otras conclusiones sobre protección de datos a la que llegan los Altos tribunales españoles son: 1) No es invocable cuando se persiguen actuaciones terroristas o de delicuencia organizada; 2) no todos los datos de carácter personal recogidos en un archivo "sensible", como una historia clínica, están protegidos constitucionalmente sino solo aquellos que estén más íntimamente conectados al ámbito de la intimidad; 3) debe acreditarse el perjuicio cuando alguien haya accedido a unos datos personales, salvo en el que caso de que éstos

sean sensibles por su vinculación con la salud, vida sexual o creencias, en cuyo caso no es necesaria la acreditación del perjuicio porque se entiende que el mero conocimiento por otra persona de este tipo de datos provoca una lesión del derecho fundamental; 4) existe una intimidad económica en la que está incluida la información fiscal; 5) la imagen personal está dentro de la intimidad y quien instale una cámara debe asegurarse de informar de los motivos que le llevan a recabar este dato de carácter personal .

6. A nivel constitucional, los aspectos que tienen mayor relevancia en relación a la ciberseguridad están relacionados con el derecho a la intimidad, la inviolabilidad del domicilio, la protección de datos y el secreto de las comunicaciones.

   Nuestro Tribunal Supremo ha tenido que diferenciar los conceptos de privacidad e intimidad, siendo el primero de ellos más amplio.

   El Alto Tribunal ha establecido doctrina sobre las interceptaciones lícitas de las comunicaciones en la actuación de Fuerzas y Cuerpos de Seguridad del Estado sobre la que destacamos: 1) exige que la policía tenga buenas razones o Fuertes presunciones para poder solicitar una autorización judicial con la cual interceptor comunicados; 2) además de la autorización judicial, se exige que la actuación policial supere el test de constitucionalidad (proporcionalidad, idoneidad y necesidad), por no existir otra posibilidad menos lesiva del derecho fundamental; 3) ha tenido que interpretar qué se entiende por tal comunicación que, por tanto, estará amparada por el derecho fundamental al secreto de las mismas, adaptando su teoría tradicional sobre el correo postal a los chat y correos electrónicos. Así, las comunicaciones que están protegidas son las que suceden en el momento de la incautación y no las que hubieran tenido lugar con anterioridad a ese momento. Además, ha tenido que enfrentarse para decidir si la localización de una dirección IP para iniciar unas investigaciones penales puede considerarse vulneración del secreto de las comunicaciones, alcanzando una respuesta negativa.

Por su parte, en cuanto a la incautación de dispositivos de almacenamiento masivo en el curso de investigaciones policiales y el volcado de sus datos, los problemas de posible injerencia en los derechos fundamentales a la intimidad y al secreto de las comunicaciones se salvan por medio de la debida autorización judicial, la cual, además, debe estar debidamente motivada.

7. En el ámbito laboral, son pocas las sentencias de nuestros Altos Tribunales que versan sobre la temática de la seguridad informática y en ellas se constata la dificultad de realizar el control o vigilancia de la actividad laboral por parte de la empresa respetuoso con el derecho a la intimidad de las personas trabajadoras. El asunto más reiterado es la colocación de cámaras de seguridad en el centro de trabajo. En este tema la jurisprudencia ya es clara al exigir: 1) que la instalación de las cámaras, salvo excepciones por la existencia de sospechas de irregularidades graves, sea pública y conocida por los trabajadores y, por tanto, que evite el "elemento sorpresivo" y permita al trabajador argumentar que no sabía que estaba siendo grabado; 2) debe ser conocido por los trabajadores que la propia finalidad de las cámaras de vídeo vigilancia, que en general, se colocan para documentar irregularidades en la empresa y 3) que el consentimiento del afectado en estos casos debe entenderse implícito en el marco de las relaciones laborales.

Para terminar, debemos indicar que el trabajo realizado puede ser continuado bien buscando y analizando sentencias de tribunales internacionales (Tribunal Europeo de Derechos Humanos o del Tribunal de Justicia de la Unión Europea), bien desarrollando la doctrina establecida sobre ciberseguridad en los juzgados y tribunales españoles inferiores, cuestión a abordar en futuras contribuciones científicas.

IX.- ANEXO

La tabla de sentencias seleccionadas se encuentra alojada en la siguiente página web:

http://hdl.handle.net/10016/33844

X.- BIBLIOGRAFÍA

CONSEJO GENERAL DEL PODER JUDICIAL, *Memoria del Tribunal Supremo 2019,* 2020*,* accesible en: https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Tribunal-Supremo/Actividad-del-TS/Memoria-del-TS/Memoria-2019-TRIBUNAL-SUPREMO

DAVARA FERNÁNDEZ DE MARCOS, E. y DAVARA FERNÁNDEZ DE MARCOS, L., *Delitos Informáticos*, Aranzadi, Cizur Menor (Navarra), 2017.

ENCILOPEDIA BRITÁNICA, https://www.britannica.com/topic/cybercrime

JIMENO MUÑOZ, J., *Derecho de daños tecnológicos: ciberseguridad e insurtech*, Dykinson, Madrid, 2019.

ONS GAMON, V., *Ciberterrorismo amenaza a la seguridad. Respuesta operativa y legislativa, nacional e internacional*, Tesis Doctoral (inédita), Universidad Nacional de Educación a Distancia (UNED), 2018, accesible en línea: http://e-spacio.uned.es/fez/eserv/tesisuned:ED-Pg-DeryCSoc-Vpons/PONS_GAMON__Vicente_Tesis.pdf

TRIBUNAL CONSTITUCIONAL DE ESPAÑA, *Memoria 2019,* 2020, accesible en: https://www.tribunalconstitucional.es/es/memorias/Paginas/default.aspx