UNIVERSIDAD MIGUEL HERNÁNDEZ

FACULTAD DE CIENCIAS SOCIALES Y JURÍDICAS DE ELCHE

GRADO UNIVERSITARIO EN SEGURIDAD PÚBLICA Y PRIVADA

TRABAJO DE FIN DE GRADO

CURSO 2021-2022

DELITOS INFORMÁTICOS

DELITO CONTRA LA INTIMIDAD

TUTOR: ÁLVARO GARCÍA DEL CASTILLO LÓPEZ

ÍNDICE

RESUMEN

La creación de nuevos sistemas de comunicación y la aparición de tecnologías que han supuesto la llegada de la *sociedad de la información y las TIC's,* supone no solo la existencia de beneficios e inconvenientes en lo que se refiere a la creación de un mundo virtual paralelo al preexistente, sino también la aparición de nuevos delitos en los que el criminal no había podido incurrir hasta ahora por la no existencia de dichos elementos.

Es imprescindible que el legislador adapte la regulación penal a la aparición de los posibles nuevos delitos que aparecieren o pudieran aparecer por dicho progreso, delitos que hasta su expresa regulación no estuvieron penados, o eran difíciles de subsumir bajo otro tipo penal.

Se dedican estas páginas al estudio del Código Penal en lo que se refiere a la regulación de los *delitos informáticos,* por lo que vamos a detenernos en su análisis y estudio desde un punto de vista doctrinal – en lo que a características y funcionamiento del propio delito se refiere-. Es también objetivo de este estudio el análisis doctrinal y jurisprudencial hecho previamente, si bien en última instancia concluimos la buena función que el legislador ha venido haciendo, así como alguna crítica hacia la regulación existente, que no es siempre completamente apropiada (*metodología de investigación y estudio bibliográfico).*

Palabras clave: *delito informático, descubrimiento y revelación de secretos, tecnología, TIC's.*

ABSTRACT

The creation of new communication systems and the emergence of technologies that have meant the arrival of the information society, not only implies the existence of benefits and drawbacks in terms of the creation of a virtual world parallel. these facts also suppose the appearance of new crimes in which the criminal had not been able to incur until now due to the non-existence of said elements.

It is essential that the legislator adapt the criminal regulation to the appearance of possible new crimes that appear or could appear for such progress, crimes that until their express regulation were not punished, or were difficult to subsume under another criminal type.

These pages are dedicated to the study of the Criminal Code in what refers to the regulation of computer crimes, so we will stop in its analysis and study from a doctrinal point of view - in terms of characteristics and functioning of the crime itself it means-. The aim of this study is also the doctrinal and jurisprudential analysis previously done, although ultimately we conclude the good function that the legislator has been doing, as well as some criticism towards the existing regulation, which is not always completely appropriate (*research methodology and bibliographic study*)

Keywords: *computer crime, discovery and disclosure of secrets, technology, TIC's.*

ABREVIATURAS

- **CE**. Constitución Española, 1978
- **CP**. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. En su última redacción, otorgada por la Ley Orgánica 1/2015, de 30 de marzo.
- **LEC**. Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.
- **LECrim**. Real decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal.
- **LO.** Ley Orgánica.
- **FJ.** Fundamento Jurídico.
- **TS**. Tribunal Supremo.
- **AP**. Audiencia Provincial.
- **TIC's.** Tecnologías de la Información y la Comunicación.
- **CENDOJ**. Buscador de jurisprudencia del Poder Judicial *(http://www.poderjudicial.es/search/indexAN.jsp)*
- **CGPJ**. Consejo General del Poder Judicial

1. INTRODUCCIÓN

La llegada de la Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal ha supuesto una serie de modificaciones en nuestro ordenamiento jurídico penal, pudiéndose hablar de una de las mayores reformas del mismo a lo largo de su trayectoria, sino la más importante.

Además de consecuencias de lo más diversas como pudieran ser la eliminación de la figura de la *falta* o la creación de nuevos delitos derivados de dicha supresión, la misma ha supuesto, también, la introducción de determinados artículos relacionados con *el delito informático*, como es el caso de los artículos 197 bis, 197 ter y 197 quater y 197 quinquies, cuyas redacciones se añaden al texto legal y entran en vigor a partir del día 1 de julio de 2015.

La llegada de las nuevas tecnologías y el progreso de las TIC's supone, al final, la inclusión en nuestro ordenamiento de diversas nuevas situaciones que en definitiva dan también lugar a nuevos ilícitos. El progreso de la tecnología supone también el progreso en las formas de cometer delitos o ilícitos en el más amplio sentido. Aunque la extensión del Código Penal permite abarcar diversidad de situaciones, lo cierto es que hasta hoy el legislador no se ha visto en la necesidad de regular, de forma específica, aquellos casos por los cuales el imputado podía haber cometido un delito de forma electrónica o a través de medios informáticos o electrónicos, aunque dichas conductas fueren subsumibles en otros tipos penales.

La creación de los *ciberdelitos*,[1] -en palabras de nuestro Código Penal *delitos informáticos*-, conlleva una novedad legislativa que abarca delitos informáticos que abarcan tan amplios campos como los derechos contra la intimidad de los artículos 197 CP y siguientes, que ya adelantábamos, o los *delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores* de los artículos 270 CP y siguientes. Si bien ambos grupos de delitos se refieren de forma especial a delitos cometidos haciendo uso de elementos informáticos, vamos a referirnos a los que se engloban, según los artículos 197 y ss., bajo el campo de los *delitos contra la intimidad, el derecho a la propia imagen y a la inviolabilidad del domicilio.*

En concreto, el artículo 197 del Código Penal se refiere a la posibilidad de que se descubran secretos o se vulnere la intimidad de cualquier individuo sin su consentimiento (delito de descubrimiento y revelación de secretos). A partir de este delito, la reforma del Código Penal que otorga la Ley Orgánica 1/2015 comienza a entender la posibilidad de que dicha revelación de secretos se lleve a cabo a través de artificios o instrumentos técnicos para obtener datos informáticos (197 bis) así como la posibilidad de que dicha revelación se lleve a cabo en el seno de organización o grupo criminal (art. 197 quater) e incluso la posibilidad de que dicha revelación se lleve a cabo por parte de una persona jurídica.

[1] El término *ciberdelito* aparece por primera vez, según Gudín Rodríguez-Magariños (2016) en la obra literaria *Neuromante*, de William Gibson, si bien su uso se ha extendido a todos los ámbitos sociales, con especial referencia al campo del Derecho.

No obstante, aunque consideramos imprescindible el análisis del artículo 197 del Código Penal en lo que se refiere a la reforma otorgada por la LO 1/2015, el presente trabajo va a hacer estudio de los delitos informáticos en lo que se refiere a toda la trayectoria que han tenido los mismos en nuestro ordenamiento, desde la inclusión que hizo el legislador al incorporarlos a nuestro Código hasta las últimas reformas que se han llevado a cabo, dada la necesidad de actualizar nuestra regulación y dar cabida a dichos supuestos.

Vamos a entender los términos *ciberdelito* y *delito informático* sinónimos, en la medida en que ambos supondrán la actividad delictiva por la cual se imputa al individuo la responsabilidad penal de los hechos cometidos a través de medios electrónicos o informáticos.

Si el ámbito de estudio de nuestro trabajo van a ser *los delitos informáticos*, tenemos que encuadrar tales delitos como resultado del progreso del *estado de la técnica*, pues si el delincuente ha cometido los delitos de forma tradicional a través de todo tipo de argucias y haciendo uso de elementos físicos tradicionales, hace uso ahora el delincuente de elementos electrónicos tan diversos como programas informáticos, *spyware*, *etc.*, tanto en su vertiente física (ordenadores) como en aquella más abstracta (programas informáticos) . Quizás una de las formas de llevar a cabo los ilícitos de la cual tendríamos que hacer especial mención es a la red de redes, *internet* que ha permitido la rápida interconexión de los delincuentes con el resto de individuos de la sociedad de forma prácticamente momentánea, permitiendo, a través de elementos característicos de la misma como *el anonimato*, llevar a cabo todo tipo de *ciberdelitos* con la voluntad de quedar impune.

Si decíamos que las ventajas de la informática y de las nuevas tecnologías de la comunicación son incuestionables, las mismas suponen de forma paralela inconvenientes a la hora de imputar el delito al reo. Véase la posibilidad de que el individuo se ponga en contacto con un sujeto de otra nacionalidad, y en consecuencia de ello que esté regido por un orden jurisdiccional distinto al de la nación española. Si el delincuente español comete ilícito contra un sujeto de otra jurisdicción, o el delincuente extranjero lo comete sobre el bien jurídico protegido bajo el campo jurisdiccional español, la resolución del conflicto se complica.

Pese a que las nuevas tecnologías han permitido un amplio avance social, con un amplio desarrollo en las últimas décadas de sectores como el de la *educación* o el *comercio electrónico*, el delincuente ha modificado sus técnicas de delincuencia para adaptarlas a dichos mecanismos. Es por ello que no entendemos que el legislador o los tribunales puedan resistirse al cambio, en cuanto la finalidad de nuestro ordenamiento no es otra que la de hacer defensa de los intereses sociales y personales, imposibilitando que el delincuente pueda inferir en la esfera del bien jurídico protegido del sujeto, o bien, cuando esta injerencia se produzca, el ordenamiento penal tenga prevista una respuesta.

Es por ello que centraremos nuestro estudio en la necesaria labor que, de forma idónea, ha realizado el legislador al incluir la redacción de los delitos informáticos dentro de sectores como el delito a la intimidad, centrándonos en dicho sector, para concluir, tras

el estudio objetivo y subjetivo del tipo penal, en una crítica hacia lo mejorable dentro de la legislación y jurisprudencia existente, así como, en su caso, un elogio a sus aciertos.

2. CUESTIONES PREVIAS

No podemos partir en el estudio del delito informático si no planteamos, en primer lugar, los objetivos generales y específicos que queremos alcanzar, así como, en su caso, cuáles serán los principios elementales y cuestiones sin las cuales no cabrá la comprensión del presente trabajo.

2.1. OBJETIVOS GENERALES Y ESPECÍFICOS

Vamos a definir así, en primer lugar, los objetivos del presente estudio.

OBJETIVO GENERAL

- El objetivo general del presente estudio será definir la regulación que nuestro Código Penal hace a *los delitos informáticos*, definiendo cuales son las principales características y requisitos que los mismos presentan a lo largo su articulado.

OBJETIVOS ESPECÍFICOS

- Analizar las cuestiones previas necesarias para la comprensión del tema.
- Definir el concepto de delito informático.
- Analizar los preceptos normativos en los que se recoge el delito informático y sus distintas vertientes.
- Determinar las características de cada artículo por el cual se defina un delito informático.
- Definir el *ciberespionaje y* la *ciberseguridad.*
- Relacionar nuestro estudio, en la medida de lo posible, con jurisprudencia por la que se desarrollan elementos fundamentales del delito informático.

2.2. ANTECEDENTES HISTÓRICOS.

A lo largo del siglo veinte y durante el desarrollo del presente siglo se ha producido una *revolución digital,* cuyas principales características son el desarrollo de la tecnología en todos sus ámbitos tanto en lo que se refiere al hardware (desarrollo y creación de nuevos sistemas informáticos en su vertiente física – *smartphones, tablets, ultrabooks-),* como en lo que se refiere a la creación y desarrollo de sofisticadas herramientas de software (programas informáticos, sistemas operativos, *spyware*, *malware*…[2]) (De Sola Quintero, 2015).

[2] Gallego Yuste (2012) define el *spyware* como aquel software espía que trabaja en la sombrar recopilando datos del usuario, con la finalidad de hacerle un envío masivo de publicidad o recopilar sus hábitos o costumbres con la única finalidad de hacer llegar esta información a empresas interesadas, a sea de forma licita o ilícita. Define el mismo autor el malware como un programa dañino cuya finalidad es modificar la conducta habitual de un programa con el fin de modificar sus funciones y sacar provecho del usuario, sin que este sea consciente de tal intrusión.

Nuestro legislador no ha venido incluyendo en nuestro ordenamiento regulación referida al *delito informático* en la medida en que el mismo ha sido inexistente a lo largo de la historia, o prácticamente inusual.

Es con la llegada de la *sociedad de la información* y de las TIC's cuando comienza a existir la necesidad de que dicha realidad social sea regulada, pues recordemos que la función del legislador no es otra que la de adaptarse al ámbito social y cultural del momento para crear un ámbito normativo que sea capaz de regular sus distintas situaciones, modificando la conducta de todo aquello que vaya en contra de los intereses de los individuos que forman parte de dicho conjunto. – y, en definitiva, del bien jurídico protegido-. Los antecedentes de los delitos informáticos van, así, a la par del desarrollo de las nuevas tecnologías y de la sociedad de la información (Loredo González, 2013)

Aunque autores como Mitchell (1996) el ciberespacio es un lugar que se rige por sus propios apoyos o estructuras, equilibrio que permite la existencia de las redes y estructuras informáticas de forma análoga al mundo real, lo cierto es que entendemos que no cabe que dicho espacio quede sin regular en la medida en que su creación y proyección está estrechamente relacionada con el mundo real, más aún en un mundo donde cada vez más los intereses reales e informáticos se difunden para crear uno solo.

Al final, la sociedad de la información conlleva una incuestionable *dependencia tecnológica* de todos los sujetos que forman parte de la misma, en la medida en que cada vez más, se ven aquellos imposibilitados para el desarrollo de sus costumbres y hábitos diarios si no es mediante el uso de dichas tecnologías y elementos informáticos (Gudín Rodríguez-Magariños, 2016). Se puede decir que ha nacido un nuevo medio que es capaz de enfrentarse a los límites de lo físico y confundir al derecho, por lo que no cabe que el legislador no adapte nuestro ordenamiento, en todos sus órdenes, a tales apariciones fundadas en la dificultad de organización e inexistencia de gobierno preexistente.

Es difícil realizar una conceptualización del delito informático en la medida en que su definición y las conductas que han de entenderse incluidas dentro del mismo son diversas y su conceptualización aún no es del todo precisa, no pudiendo acotarse realmente el campo de conductas incluidas bajo dicha tipología de delito (Hernández Díaz, 2009). Una de las causas de esta dificultad de conceptualización es la diversidad de elementos que forman parte de este campo de estudio, así como la celeridad con la que los mismos aparecen, e incluso desaparecen. Es fácil comprobar como cualquier tipo de *software* o *hardware* que a fecha de la redacción del presente trabajo suponga una incuestionable novedad será pronto sustituido por otro de mejores o similares características, por lo que es posible, e incluso nos atrevemos a calificar como indiscutible, que los delitos que analizamos en estas páginas quedarán relegados a estudios históricos o precedentes de las futuras actualizaciones que llevará a cabo el legislador penal.

El 27 de noviembre de 2009, el gobierno de la nación española lanzaba un proyecto de reforma de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, cuyo principal objetivo no era otro que el de plasmar en nuestro ordenamiento las directivas comunitarias en materia de regulación del derecho informático, colmando las

lagunas que hasta ahora habían venido surgiendo en la práctica jurídica por la ineficacia del articulado previsto.

Se introdujeron así, a partir de la Ley Orgánica 5/2010 los delitos informáticos en nuestro ordenamiento, los cuales quedaban plasmados en normas que protegían la confidencialidad y la integridad y disponibilidad de datos y sistemas informáticos (Salvadori, 2011). Pese a que hasta la llegada de dicha ley no se podía hablar de existencia de *delitos informáticos* en sentido propio dentro de nuestra regulación penal, podemos confirmar que era posible aplicar, y así se venía haciendo, determinados preceptos penales haciéndolos extensibles al ámbito informático, por la falta de normas específicas. De hecho, incluso algunos autores llegaron a calificar irrelevante la necesidad de introducir nuevas conductas que englobaran los delitos informáticos, por ser posible incluir las mismas dentro de las intrusiones ilícitas en bienes jurídicos protegidos que ya se encontraban reguladas por nuestro Código Penal: es el caso, por ejemplo, de la irrelevancia de regular una disposición específica sobre el hacking[3]. Según Casabona (2006) y Rueda Martín (2008), la intromisión ilícita en un sistema informático ajeno podía ser castigada *en cuanto conducta instrumental a la comisión de determinados delitos informáticos, en particular los delitos de forma libre* (Salvadori, 2011, p.228).

Los tipos penales existentes en el Código Penal original de 1995 fueron ampliados así de dos formas: creando en primer lugar subtipos de delito dentro de los delitos existentes, y ampliando en segundo lugar el ámbito de los objetos materiales de los delitos que presentaban analogía con los calificados como nuevos delitos. (Salvadori, 2011). Se creaba así una distinción entre *delitos informáticos* cuando los mismos constituyen objeto material del delito y *delitos informáticos* que son instrumento para la comisión del delito (González Rus, 1999).

Así, y aunque no quepa duda de la diferenciación entre los delitos cometidos a través de la informática cuando la misma supone medio idóneo para la relación del delito y aquellos en que la informática es objeto del mismo, algunos autores se atreven a incluir una tercera categoría: los delitos cometidos *contra y a través* de un sistema informático, e incluso una cuarta categoría que englobase los delitos contra la propiedad intelectual cuando los mismos sean de naturaleza informática (Hernández Díaz, 2009).

Con posterioridad a dicho acercamiento de nuestro ordenamiento jurídico penal al campo del *ciberdelito*, prestará especial relevancia la Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica el Código Penal de 1995. A través de esta reforma se introducen nuevos elementos a nuestro Código de forma análoga a lo que ya hacía la Ley Orgánica 5/2010, introduciéndose nuevas referencias y regulación del delito informático en lo que ahora los interesa, en los artículos 197 CP, 197 bis, 197 ter, 197 quater y 197 quinquies, añadiéndose de forma totalmente plena la redacción de los cuatro últimos, y produciéndose también una actualización del primero de los artículos citados. La modificación de la que hablamos, publicada el 31 de marzo de 2015, entra en vigor y comienza a surtir plenos efectos en nuestro ordenamiento el 1 de julio de 2015.

[3] Se entiende por *hacking* a la intromisión ilícita en un sistema informático ajeno por parte de un cibercriminal (Salvadori, 2011).

2.3. LA PRUEBA ELECTRÓNICA

Aunque escapa de la regulación de los artículos 197 y siguientes del Código Penal, queremos hacer referencia a otro de los elementos que, de forma paralela al delito informático y haciendo uso de fundamentación jurídica y doctrinal muy similar, ha conseguido consagrarse en nuestro ordenamiento a lo largo de las últimas tres décadas: *la prueba electrónica.*

Este acercamiento entre los conceptos de prueba electrónica y delito informático lo hacemos en cuanto ambos suponen una afectación genérica de los derechos y principios constitucionales, afectación que siempre ha de hacerse a favor del progreso de ambos campos (derecho y tecnología). En este sentido Roig Batalla (2011), para el cual:

"El jurista debería acercarse sin complejos a esta propuesta multidisciplinar de estudio de las libertades informativas, si de verdad quiere complementar la protección jurídica de derechos fundamentales con el también apasionante mundo de la tecnología […]".

La incorporación de las nuevas tecnologías al sistema judicial y a su procedimiento son paralelas a la inclusión de los delitos informáticos en nuestro Código Penal, por lo que vemos que la cercanía temporal entre ambas inclusiones supone, al final, la aceptación del uso de las tecnologías de la información y la comunicación en nuestro ordenamiento jurídico penal – y en cualquiera de los demás ordenes-. La incorporación de las nuevas tecnologías al sistema judicial y a su procedimiento proceden, de forma concreta, de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, por la que se ha venido experimentando un continuo impulso motivado, al igual que en el propio delito informático, por las exigencias de diversas directivas europeas[4].

Una de las directivas que mayor alcance ha supuesto en lo que se refiere a la trasposición de sus elementos hacia nuestro Código Penal es la Directiva 2013/40/UE, del Parlamento y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información. No obstante, dicha decisión es también consecuencia de la voluntad del propio legislador en dar una solución a aquellas actitudes que supongan la divulgación de imágenes o grabaciones contraviniendo la voluntad del afectado, incluso aunque las mismas se hubieran obtenido con el consentimiento del propio afectado. Dicha directiva se verá más tarde complementada por otras de similar alcance, como es el caso de la Directiva (UE) 2016/1148, de 6 de julio, sobre seguridad de las redes y de la información, cuya finalidad no es otra que la de llevar a cabo una coordinación entre los Estados miembros de la UE en lo que al uso ilícito de internet se refiere.

No podemos dejar pasar por alto tampoco la relevancia que la *prueba electrónica* y el *delito informático* aportan al procedimiento en el orden jurisdiccional penal, en el

[4] La Ley 18/2011 reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia supone una incorporación, según el prólogo de la misma ley, al Plan de Acción E-Justicia-, en el que se busca la mejora de la eficacia de los sistemas judiciales, así como la cooperación entre las autoridades judiciales y la adopción de medidas coordinadas a nivel nacional y europeo.

cual ha disminuido de forma directamente proporcional la aparición de otras formas de comunicación distintas a las que otorgan los medios digitales (Betrán Pardo, 2015).

Se consolida así la *prueba electrónica o prueba digital* como un nuevo medio de prueba de los que nuestro artículo 299.2 de la LEC venía recogiendo, a través de la *cláusula de numerus apertus*[5] que el mismo precepto contiene, la posibilidad de que dentro del proceso judicial penal se utilice como medio de prueba cualquier instrumento probatorio distinto al que la propia ley recoge de forma expresa, clausula reiterada por la regulación del artículo 299.3 LEC. Así lo entiende Betrán Pardo (2015), para la cual, aunque no existe en nuestra Ley de Enjuiciamiento Criminal alusión expresa a los medios de prueba que estamos tratando, no existe obstáculo para acudir a una norma de relativa novedad y de aplicación subsidiaria, como es la Ley de Enjuiciamiento Civil.

Definiremos así la prueba electrónica como *"toda información de valor probatorio contenida en un medio electrónico o transmitida por dicho medio".* (Sanchís Crespo, 2012, p. 713), entendida dentro de un sistema de medios de prueba abierto que permite de forma implícita la inclusión de un medio de prueba digital en su carácter más amplio, sistema de medios de prueba que se ha alcanzado gracias a la regulación comunitaria y nacional que aboga por la inclusión en nuestro orden social y jurídico de los avances y medios tecnológicos.

3. EL CONCEPTO DE DELITO INFORMÁTICO

No podemos partir del presente estudio si no hacemos primero un análisis introductorio de qué debe entenderse por *delito informático.* Como decíamos unos párrafos más atrás, y aunque cabría hacer precisiones a esta afirmación, vamos a utilizar a lo largo de nuestras páginas los términos *ciberdelito y* delito informático como equivalentes. También vamos a recoger las definiciones que entendemos más afines a nuestro entendimiento partiendo de bibliografía diversa para concluir redactando nuestra propia definición.

Antes de adentrarnos en el concepto de *ciberdelito o delito informático,* queremos englobarlo dentro de un campo de estudio que calificaremos como el derecho informático, que forma parte ahora de nuestra regulación penal en la medida en que se ha producido el avance de la sociedad de la información. Así, Hernández Díaz (2009) habla del "*Derecho informático*" como el *conjunto de normas jurídicas que regulan la utilización de los bines y servicios informáticos en la sociedad* (p. 227). Si el derecho informático se forma por el conjunto de normas que regulan la utilización de los elementos informáticos que forman parte del conjunto social, no hay duda de que se ha de entender por delito informático al hecho doloso que se realiza haciendo uso de los dispositivos informáticos que el autor del delito considere oportunos en cada momento.

García de la Cruz (2009) define el delito informático como *toda acción culpable realizada por un ser humano que cause un perjuicio a personas sin que necesariamente*

[5] Esta cláusula de *números apertus* se enfrenta a opiniones de autores para los cuales tanto el Código Penal como la LECrim enumeran una serie de medios de prueba englobados bajo el *números clausus*, en la medida en que no cabe interpretación más allá de lo estrictamente técnico recogido de forma expresa en la regulación de los medios de prueba (Aige Mut, 2014)

se beneficie el autor o que por el contrario produzca un beneficio ilícito a su autor, aunque no perjudique de manera directa o indirecta a la víctima […] siempre que […] se tenga a las computadoras como instrumento o fin, o que la computadora esté involucrada *como material objeto o como medio* (p. 6). Extraemos de esta definición varias características del concepto de dicho delito (De Sola Quintero, 2015):

- Puede provenir de *acción u omisión.* Dicen algunos autores, que ha de tratarse de un *acto humano* (De Sola Quintero, 2015).
- El acto ha de perjudicar directa o indirectamente a la víctima: ha de tratarse de un hecho antijurídico.
- Conforme al principio de legalidad del artículo 25.1 CE consagrado en los dos primeros artículos del Código Penal, no puede castigarse la acción u omisión si la misma no está prevista explícitamente como delito por la propia ley[6],
- Ha de conllevar un elemento de *culpa,* en cuanto cabe que al sujeto se le impute tanto un elemento de dolo (intención) como de culpa o negligencia.
- El elemento informático puede estar involucrado en el delito como objeto material, como medio, o como fin del propio delito.

Nos atrevemos así a elaborar una definición propia, por la que entendemos el delito informático como la acción u omisión criminal que provoque un beneficio o interés directo o indirecto en el autor o un tercero, siempre que para su consecución se haya hecho uso de un medio o programa informático o electrónico, en su más amplio sentido. De este modo, entenderemos que el medio o programa informático puede tenerse en cuenta como *instrumento* o como *fin* de la conducta típica recogida como delito.

Los delitos informáticos pueden atender a distintas clasificaciones, como pudiera ser la diferenciación según aquellos que supongan *ataques que se producen contra el derecho a la intimidad* frente a las *infracciones a la Propiedad Intelectual* a través de la protección de los derechos de autor, si bien – siendo los dos grupos anteriores los más relevantes-, cabe incluir también dentro de este campo de estudio, por la posibilidad de cometer las infracciones penales haciendo uso de los medios o elementos informáticos, las *falsedades, los sabotajes informáticos, las amenazas, los fraudes o las calumnias e injurias*, entre otros (Estévez Martín, 2010). Entendemos que, al final, el legislador optará por incluir en el Código Penal una cláusula general extensible a todo delito, pues no cabe que en un tiempo de progreso determinados delitos puedan cometerse mediante medios informáticos y sin embargo otros puedan quedar al alcance de dicha tecnología.

Pese a que, como decíamos, el delito informático es consecuencia de un progreso digital que ha traído diversidad de ventajas en el desarrollo de nuestra vida diaria, la intangibilidad de la información que proporciona conlleva, al final, la partida de una serie de desventajas. En este sentido Davara (2004), para el cual "[…] *el desvanecimiento de teorías jurídicas tradicionales como la relación entre acción, tiempo y espacio; el anonimato […]* o *[…] la dificultad de recolectar pruebas* […] suponen, al final, una serie

[6] De ahí la necesidad que hemos citado de que el legislador incluya en nuestra regulación un amplio abanico de *delitos informáticos.*

de impedimentos que ralentizan la posibilidad de proporcionar una eficaz respuesta jurídica penal al cibercriminal.

Realmente, entendemos que la ley no ha creado, en realidad, un delito informático. Lo que ha hecho ha sido añadir, a delitos ya existentes, la posibilidad de cometer sus actos u omisiones antijurídicos de forma electrónica, o, dicho de otro modo, ha llegado el legislador a incluir *subtipos* de delito, pudiendo afirmarse que es posible cometer los mismos en su vertiente digital o electrónica, haciendo uso de instrumentos o medios digitales, pero en ningún caso creando un delito que se englobe bajo el encabezamiento del *delito informático.* Entendemos así que, aunque en el presente trabajo hablamos y hablaremos del *delito electrónico* o *ciberdelito* como una figura abstracta de la cual subyace la posibilidad de cometer un ilícito de forma digital, lo cierto es que cierta figura en realidad no existe, y que, existiendo, lo hace de forma global, incluyendo dentro de sí mismo una serie de delitos que tienen naturaleza propia por sí mismos.

Queremos referirnos también a la inclusión que hace en nuestro ordenamiento penal, la reforma del Código Penal del año 2010 citada en las anteriores páginas, en lo que se refiere al hasta entonces vigente principio *societas delinquere non potest* (Salvadori, 2011).

El artículo 31-bis CP vino recogiendo ya en 2010 la posibilidad de que a las personas jurídicas se le impute responsabilidad penal, inspirándose la redacción de dicho precepto en la denominada por la doctrina como *responsabilidad vicarial* (Quintero Olivares, 2010). Aunque dicha decisión legislativa supuso una incuestionable mejora de la defensa del orden social, lo cierto es que la auténtica inclusión de la responsabilidad social que se puede imputar a la persona jurídica en el ámbito del derecho informático aparece con la llegada de la Publicada la Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica el Código Penal.

La LO 1/2015 reafirma, en su artículo 197 quinquies, la posibilidad de que la persona jurídica, de acuerdo a la regulación del artículo 31 bis, sea responsable de los delitos comprendidos en los artículos 197 CP, 197 bis, 197 ter. Deja fuera de la regulación expresa del artículo 197 quinquies CP la referencia al artículo 197 quater, en cuanto el mismo se refiere a la posibilidad de aplicar la pena superior en grado a la organización o grupo criminal que hubiere llevado a cabo alguno de los hechos descritos en el analizado capítulo.

Nos encontramos así con un delito que podrá ser cometido tanto por parte de una persona física como, en su caso y por la redacción que otorga el artículo 197 quinquies de la vigente redacción del Código Penal, por cualquier persona física, en cuyo caso se aplicará la pena superior en grado.

3.1 EL BIEN JURÍDICO PROTEGIDO EN EL DELITO INFORMÁTICO

Como hemos adelantado en el punto anterior, el legislador no ha incluido, pese a las sucesivas reformas, un delito autónomo por el que se pueda diferenciar el delito informático en sí. El *delito informático* aparece, en realidad, como subtipo de otro tipo de

delitos que ya estaban por sí mismos consagrados en la regulación que nuestro legislador hizo con la llegada de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Sin embargo, vamos a hacer estudio de esta figura en un sentido abstracto – como si el delito informático realmente existiese-, para dar lugar después al análisis y la interrelación de dicho delito con el expresamente consagrado *delito de descubrimiento y revelación de secretos* de los artículos 197 y siguientes, en lo que se refiere a delitos contra la intimidad.

Dada la difusión del precepto y la dificultad para delimitar sus características – por la abstracción que decíamos- se puede afirmar que la concreción del bien jurídico protegido de este delito puede variar en función de la corriente doctrinal por la que se opte. Así, mientras gran parte de la doctrina afirma la necesidad de la creación de un tipo penal autónomo que regule las conductas informáticas, otra se limita a hacer estudio de los tipos existentes como si de un delito con naturaleza propia se tratase.

De ahí que, en ocasiones, más que hablarse de un delito informático, algunos autores se refieran a términos como *delincuencia informática* o incluso a *delitos informáticos* en su vertiente más plural, eludiéndose, en la medida de lo posible, el término *delito* por la limitación que dicha acotación supondría en el estudio del mismo (Hernández Díaz, 2009).

Así, autores como Hernández Díaz (2009) diferencian bienes jurídicos protegidos como la seguridad informática, la integridad, confidencialidad y disponibilidad de los datos y sistemas informáticos, o la intimidad. Sin embargo, entendemos que tal bien jurídico habrá de adaptarse a las circunstancias de cada delito, por lo que preferimos no delimitar así el ámbito del bien jurídico protegido del delito informático, por el progresivo avance que, tenemos por seguro, va a suponer la regulación de tal delito en nuestro ordenamiento.

Para autores como Acurio del Pino (2008), el bien jurídico protegido en el delito de informático se extiende, en realidad, a la información misma como bien jurídico que ha de ser objeto de protección, en cuanto la misma supone una fuente de valores inmateriales que, a su vez, suele verse plasmada en cuatro tipos de bienes jurídicos, en función del delito tradicional con el que se interrelacione:

- El patrimonio.
- La intimidad y confidencialidad de los datos.
- La seguridad del tráfico jurídico.
- El derecho de propiedad, en cuanto al sistema informático físico que es afectado por algún tipo de daños.

Hacer también especial referencia a la opinión de Quintero Olivares (2001), para quien el bien jurídico protegido del delito informático es, en realidad, internet – entendido como la red a la que están sujetas todas las transacciones informáticas y que es objeto del ilícito cuando el mismo se lleva a cabo.

No cabe duda así de que el bien jurídico protegido se puede entender según distintas vertientes por la ya citada difusión del propio delito que, como decíamos, ni el legislador ha llegado a concretar. Nos interesa pues, a efectos del estudio del siguiente apartado, el bien jurídico protegido por el cual se afecta al derecho a la intimidad, que recordemos está protegido por el artículo 18 de la CE.

3.2 ANÁLISIS SUBJETIVO DEL TIPO PENAL

Si teníamos ciertas dudas en la delimitación del concepto del delito informático y en su extensión al bien jurídico protegido, las mismas se dispersan cuando tenemos que diferenciar los sujetos que forman parte del tipo penal.

Se consagra como *sujeto activo* aquel individuo que comete el delito de tipo informático, sujeto que suele coincidir (aunque no ha de atenderse a esta calificación de forma totalmente exclusiva) con sujetos cuya especial habilidad para el control de sistemas informáticos le permite sacar provecho de la misma para plasmarla en el acaecimiento de un delito (Rivera Panizo, 2009).

En el mismo sentido Acurio del Pino (2009), para el cual los sujetos activos que cometen el delito informático *no presentan el denominador común de los delincuentes*, pues frente a las habilidades del delincuente tradicional, el que comete el delito informático tiene habilidades para manejar sistemas informáticos, y en gran parte de las ocasiones su relación laboral le permite tener acceso o control de información sensible que le facilita la comisión del delito. Así se refiere Acuario del Pino (2009) al informe del Manual de las Naciones Unidas para la prevención y control de delitos informáticos, en el que se diferencia de forma expresa la posibilidad de que los delitos informáticos sean realizados desde dentro de la propia empresa (*insiders)* o conforme a una actividad delictiva externa (*outsiders*).

Tampoco hay dudas en la consagración del *sujeto pasivo* del delito, que se corresponderá con el titular del bien jurídico protegido, según entendamos que el bien protegido es uno u otro – refiriéndonos así a las distintas opciones que dábamos en los apartados anteriores-

En concreto, Rivera Panizo (2009) habla del sujeto pasivo del delito informático como la *persona física o jurídica que utiliza sistemas automatizados de información, normalmente a través de internet*[7]. Habitualmente, los sujetos pasivos del delito no llegan a mostrar la comisión del mismo al no denunciar los hechos informáticos, bien por no saber que el ilícito constituye delito y que su hecho está amparado por el ordenamiento jurídico, bien por decisión propia.

4. ESPECIAL REFERENCIA A LA MODIFICACIÓN DEL DELITO DE DESCUBRIMIENTO Y REVELACIÓN DE SECRETOS

[7] La referencia que esta autora hace al término *internet* nos recuerda al bien jurídico protegido que consagraba Quintero Olivares (2001).

Como adelantábamos en páginas anteriores, vamos a centrar nuestro estudio en la figura del delito de descubrimiento y revelación de secretos de los artículos 197 y siguientes del vigente Código Penal, así como las modificaciones que los mismos han sufrido a lo largo de las reformas de nuestro Código. Se puede afirmar que son serias las dificultades que nuestra doctrina y jurisprudencia han encontrado al intentar delimitar los dos tipos básicos de descubrimiento y revelación de secretos, así como sus correspondientes subtipos agravados, en la medida en que su definición es a veces similar o poco concreta, y el estudio ha de ser profundo para poder concluir las características diferenciadas de cada redacción concreta (Montserrat Sánchez-Escribano, 2017).

El artículo 197 CP recoge, en su redacción original dada por el Código Penal de 1995, la posibilidad de que un sujeto se apropiare de *papeles, cartas, mensajes de correo electrónico* o cualquier otro documento o efecto personal, interceptare *sus telecomunicaciones,* o utilizare *artificios de escucha, transmisión, grabación […]* u otros artificios de análoga naturaleza con la finalidad de descubrir secretos o vulnerar la intimidad de otro (sin su consentimiento) fuese penado con la pena de prisión prevista en el propio artículo.

Se puede hablar así de dos delitos distintos dentro del artículo 197.1 CP: *el apoderamiento de documentos y efectos personales,* en primera instancia, y *la obtención ilícita cualquier señal de comunicación (sonido, imagen, video…),* en segunda. Recordemos que ninguno de estos dos delitos ha sufrido modificación ni alteración en su redacción, quedando, en palabras de González Collantes (2015), *incólumes* en lo que a su redacción se refiere.

Entiende González Collantes (2015) que, pese a haber quedado intactas las redacciones de los artículos 197.1 CP y 197.2 CP, sí que deberían haber sufrido una modificación léxica y sustantiva en lo que a solucionar la posible falta de tipicidad que el propio artículo 197.1 CP plantea, para superar, al final, aquellos casos que pudieran quedar impunes por la redacción del citado precepto legal, así como una modificación del termino *reservado* del artículo 197.2 CP, el cual supone una interpretación según la cual el perjudicado ha de ser un tercero distinto al titular de los datos objeto del hecho criminal, mientras que en el caso de que exista un acceso no autorizado o los mismos conlleven una alteración o utilización, el perjuicio cabe tanto sobre el titular de los datos como sobre el tercero (González Collantes, 2015).

Del mismo modo impone pena el apartado segundo a aquel que se apoderare, hiciese uso o modificación de datos de carácter personal que se hallasen registrados en ficheros o soportes informáticos, electrónicos o telemáticos o en cualquier otro tipo de registro público o privado, así como quien alterase dichos datos o los utilizara en perjuicio del titular o del tercero. Aunque el artículo 197.2 CP se refiere al descubrimiento de secretos *en soporte electrónico o cualquier otro medio,* para algunos un tipo básico de *abuso informático sobre datos reservados de carácter personal* (Barreiro, 2016).

En este sentido hacer referencia al elemento de apoderamiento, que se recoge tanto en el artículo 197.1 CP como en el artículo 197.2 CP. Dicho elemento ha sido definido,

entre otras, por la Sentencia del Tribunal Supremo 4054/2015, de 6 de noviembre de 2015[8]. Según esta sentencia:

"Se apodere se ha interpretado por un sector doctrinal en sentido estricto como el apoderamiento que precisan los delitos contra el patrimonio. Otro sector se inclina por una interpretación más amplia, comprendiendo los supuestos en que se copian los datos, dejando intactos los originales o simplemente se capta, se aprehende, el contenido de la información, acepción en la que "apoderarse" resultaría equivalente a acceder al dato que se castiga también en el inciso final […]"

Interpreta así el Tribunal Supremo haciendo diferenciación a dos conceptos: el que aboga por un sentido más estricto, para los delitos contra el patrimonio, y el que lo hace por una interpretación más amplia, para los casos en los que se hace copia de datos, captación o aprehensión del contenido de la información, a través de un simple acceso que no tiene por qué suponer hacerse de forma estricta con los datos para sí mismo en un sentido más concreto. Esta diferenciación se enfrenta en realidad a la definición que hacen algunos autores, según los cuales no cabe que los datos personales sean apoderados y hacen propuesta de verbos alternativos. En este sentido Fernández-Delgado (2009). Para Romeo Casabona (2002), si el objeto material del delito puede llegar a ser un correo electrónico, no se entiende que dicho verbo requiera de una *interpretación espiritualizada.*

La misma sentencia diferencia también el concepto de *apoderamiento* con los de *utilización* y *modificación,* en cuanto ambos suponen también una injerencia en el articulado de dichos artículos: refiriéndose la utilización al uso sin el apoderamiento, y a la modificación a la alteración de los mismos tanto para mejorarlos como para perjudicarlos.

Si bien los dos primeros delitos que afectan a la revelación de datos de la intimidad personal del artículo 197 CP se refieren a *tipos básicos*¸ lo cierto es que el resto de apartados del mismo artículo (197.3 CP, 197.4 CP, 197.5 CP, 197.6 CP) recogen en realidad *tipos agravados,* salvo el artículo 197.7 CP que se podría calificar, en su caso, como un tipo específico referido a la difusión de imágenes o grabaciones obtenidas sin autorización. En concreto, los tipos agravados del artículo 197.3 CP y siguientes se concretan en:

- El tipo agravado de difusión, revelación o cesión de datos reservados a terceros (art. 197.3 CP). Autores como Barreiro (2016) entienden que dentro de este mismo artículo se recoge también un *tipo básico de revelación* que es autónomo a la figura citada, en la medida en que se describe la conducta por la que se lleve a cabo dicha difusión o revelación *sin haber tomado parte en su descubrimiento.* Se deben calificar así los delitos de difusión y de revelación de secretos autónomos, pues si la primera se consolida como tipo básico, la segunda supone la revelación de tal información sin haber intervenido en su hallazgo.

[8] ID CENDOJ 28079120012015100541

- El tipo agravado de las personas encargadas o responsables de los ficheros o soportes, para la cual han de hacer uso no autorizado de los datos personales de la víctima. (art 197.4 CP). Se consolida así este artículo como un tipo agravado con dos requisitos, en cuanto no bastará con que el hecho antijurídico sea cometido por la persona encargada o responsable del fichero[9]

- El tipo agravado de revelación de datos relativos a la *"ideología, religión, creencias, salud, origen racial o vida sexual",* para el caso especial de que los mismos tuviesen origen en una persona discapacitada (por lo sensible de la propia naturaleza de dicha información). Recoge este apartado la imposición de la pena prevista en su mitad superior. (art. 197.5 CP).

- Tipo agravado para los casos en que los hechos descritos en el artículo analizado fuesen realizados con fines lucrativos, para el cual se recoge, al igual que en el caso anterior, la imposición de la pena prevista en los apartados 1 a 4 del mismo artículo, en su mitad superior. Para autores como Nitoiu Soto (2018), la diferenciación de este tipo agravado tiene su origen en el especial desvalor de la conducta.

- Tipo agravado del artículo 198 CP, que, si bien no ha sido introducido con posterioridad a la LO de 1995, lo cierto es que ya venía recogiendo la posibilidad de que todos los delitos del artículo 197 – aplicable así, ahora, a las nuevas conductas introducidas- sea aplicable a la autoridad o funcionario público que las realizare haciendo uso de su cargo, para lo cual se prevé la aplicación de la pena en su mitad superior, así como la correspondiente inhabilitación absoluta por el tiempo determinado en el propio precepto.

Además del tipo penal del artículo 197 y las variantes que antes analizábamos, la redacción otorgada a nuestro Código Penal por la LO 1/2015 supuso la inclusión de otros tres tipos penales (arts. 197 bis apartado primero, 197 bis apartado segundo y 197 ter), así como la introducción de los tipos agravados de los artículos 197 quater CP y 197 quinquies CP. En concreto, podemos resumir dicha redacción otorgada de la siguiente forma:

- Delito de acceso sin autorización al sistema de información (art. 197 bis apartado primero CP).

- Delito de interceptación no autorizada de transmisiones no públicas de datos informáticos (art. 197 bis apartado segundo CP).

[9] Nuestro Código se refiere de forma expresa a una *fórmula de alternatividad*, en cuanto el propio artículo formula que los hechos descritos serán castigados con la pena de prisión de tres a cinco años cuando se cometan por dichas personas *"o"* se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima. Si bien entendemos que la formulación de este precepto es la de proteger a la víctima bajo un amplio abanico de supuestos, lo cierto es que dicha cláusula de alternatividad podría plantear ciertos problemas interpretativos, pues cabe preguntarse si es posible que el tipo agravado sea aplicado cuando se den ambos supuestos (aunque por la naturaleza del propio tipo agravado no cabe duda, quizás fuese relevante aclararlo en la redacción).

- Delito de facilitación de programa informático o claves o códigos de acceso con la finalidad de acceder a la totalidad o parte fraccionada de un sistema de información. (art 197 ter CP).

- Tipo agravado por haber cometido los hechos analizados *en el seno de una organización o grupo criminal* (art. 197 quater). Dicho tipo agravado es aplicable a todas las conductas analizadas con anterioridad.

- Especial referencia al acaecimiento del delito cuando la comisión se produzca por parte de una persona jurídica, en virtud de lo establecido en el artículo 31 bis del Código Penal (art. 197 quinques). Dicho artículo ha de verse encuadrado de forma conjunta al artículo 200 CP, que ya en su redacción de 1995 incluía la posibilidad de aplicar las conductas del capítulo a aquel que *"descubriere, revelare o cediere datos reservados de personas jurídicas"* sin el consentimiento de los representantes de las mismas.

Podemos concluir así que la LO 1/2015 ha producido, en primer lugar, una nueva organización de los preceptos por los que se regula el citado delito, para dar lugar así a la incorporación de nuevos delitos, que ya definíamos antes como subtipos del tipo penal principal del artículo 197 CP. Aunque decíamos páginas más atrás que uno de los principales motivos en que podíamos fundar tal modificación legislativa era la influencia comunitaria otorgada por las Directivas de la Unión Europea, lo cierto es que la doctrina venía haciendo petición de tales reformas, tal y como ya propuso en varias ocasiones el Consejo General del Poder Judicial[10] (González Collantes, 2015).

5. EL CIBERESPIONAJE Y LA CIBERSEGURIDAD

Si entendemos el espionaje la actividad consistente en conocer de forma *ilícita o encubierta* datos o hechos confidenciales de fuentes terceras[11], tenemos que ser conscientes de que, lejos de la utilización de esta práctica durante estrategias militares acontecidas en conflictos bélicos como la Segunda Guerra Mundial, sigue existiendo en la actualidad en forma digital. Si hemos venido utilizando a lo largo de estas páginas el prefijo *ciber* para referirnos a la digitalización de cualquier ámbito, qué duda cabe de la posibilidad de que el campo de la práctica del espionaje sea cubierto bajo dicha digitalización.

Recordemos que el *cibercrimen* hace referencia, tal y como ya definía Hernández Díaz (2009), a *el conjunto de conductas relativas al acceso, apropiación, intercambio y puesta a disposición de información en redes telemáticas, las cuales constituyen su entorno comisivo, perpetradas sin el consentimiento o autorización exigibles o utilizando información de contenido ilícito, pudiendo afectar a bienes jurídicos diversos de naturaleza individual o supraindividual* (p. 236).

[10] Así, por ejemplo, el informe emitido por el CGPJ sobre el Anteproyecto de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
[11] Definición propia.

El *ciberespionaje* ha de verse directamente relacionado con el concepto de *amenaza*, entendiéndose la misma como la potencial posibilidad de recibir un ataque, que en el campo virtual se verá plasmada en cualquier tipo de aprovechamiento de vulnerabilidades electrónicas (ataque de *gusanos, hacking, ataques DoS, botnets…*[12]) (Puime Maroto, 2009).

Si existe una amenaza -más bien una *ciberamenaza*-, y la misma se plasma en el ámbito del espionaje o *ciberespionaje*, es habitual que tales hechos se produzcan, por la propia naturaleza de sus elementos, de forma ilícita. Es aquí donde entra en juego la necesidad de que el acaecimiento de ilícitos penales relacionados con el ciberespacio tenga respuesta por parte de nuestro ordenamiento jurídico.

No cabe que un acontecimiento que *en la vida real* [13]consideramos ilícito, quede sin respuesta en la medida en que lesione un bien jurídico protegido, pues qué duda cabe de que el mismo suele ser real, pese a que no se plasme en un elemento físico. Como decíamos ya a lo largo de las páginas del presente trabajo, el campo digital no ha de quedar exento de la regulación por parte del ordenamiento jurídico -más aun en una sociedad que cada vez más tiende a la dependencia de lo digital- pese a la oposición de algunos autores.

Para el logro de la distribución e implementación de las herramientas digitales que los criminales vienen utilizando, se viene haciendo uso de *mensajes no deseados y sitios web infectados* (Puime Maroto, 2009). Si un ordenador se convierte en *víctima*, es porque un sujeto activo ha llevado a cabo cualquier tipo de conducta, normalmente también haciendo uso de medios electrónicos o digitales, con la finalidad de afectar al bien jurídico protegido del que es titular el sujeto pasivo del delito. El avance de los servicios disponibles y de la red de redes –*internet*- –véase la reiterada e incuestionable actividad diaria de la mayor parte de la población en todo tipo de blogs, foros, webs multimedia de audio y video o redes sociales- ha llevado al final al éxito de la ciberdelincuencia. (Puime Maroto, 2009).

Es importante concienciar a la población de la debilidad de todo tipo de sistema de seguridad, pues si bien son innumerables los beneficios y ventajas que el uso de *software* y *hardware* otorgan, los más modernos métodos de transferencia de datos y de comunicación otorgados por las TIC's suponen también un amplio elemento de vulnerabilidad, creando nuevas situaciones que hasta ahora no eran comprensibles por su dificultad de llevarse a cabo en una organización espacio temporal que aún no había llegado al actual grado de difusión.

[12] El término *gusano* hace referencia a un programa diseñado para distribuirse rápidamente a lo largo de diversas computadoras de forma ilícita; el *hacking* entendido como el estudio de los sistemas informáticos con la finalidad de aprovecharse, de forma didáctica, de sus vulnerabilidades (Martínez Alarcón, 2006); el *ataque DoS* y las *botnets* como los ataques cuya finalidades son aprovecharse del ancho de banda de la red victima para colapsar la información o utilizar los ordenadores ajenos mediante el control ilícito con la misma finalidad, respectivamente.

[13] Cuando hablamos de la vida real lo vamos a hacer simplemente equiparándola *al plano físico*, pues entendemos que no cabe calificar de irreal lo digital por el mero hecho de no plasmarse en su totalidad en lo material.

Muestra de esta posibilidad de convertir ventajas en vulnerabilidades, el estudio de la Asociación de Internautas *"El vigilante vigilado",* en el que dicha asociación presenta en septiembre de 2008 un informe por el que se pone de manifiesto que más del sesenta por ciento (60%) de las cámaras de seguridad instaladas en hogares particulares están conectadas a internet a la vez que abiertas, por lo que el acceso a las mismas desde cualquier otro ordenador es relativamente sencillo, sin que sea necesario para ello tener grandes conocimientos de informática o infringir situación jurídica calificada como delito[14].

Basta con que haya una falta de información o de conocimiento del sujeto pasivo del delito para que el mismo, dada su inconsciencia o involuntariedad, propicie por sí mismo el delito. Véase el caso en el que un sujeto, intentando descargar un documento –libre de derechos de autor o habiendo obtenido autorización para el uso del mismo-, pulsa en el botón equivocado e instala en su ordenador una aplicación maliciosa que provoca que, sin que el sujeto lo sepa, su ordenador sea incluido en una *botnet* y a través del mismo se comience a cometer todo tipo de ilícitos en nombre del propio afectado por el ilícito.

Véase también el ejemplo del panadero al que se le instala *el virus de la policía*[15] en el ordenador donde lleva al día la contabilidad de su empresa y, creyendo que eran los cuerpos policiales los que le exigían el pago de una cantidad en determinada cuenta bancaria o *bitcoin wallet*[16], procedían al pago de considerables cantidades de dinero, que llegaba en realidad a los bolsillos de los *hackers* que habían infectado el ordenador del afectado.

Ilustración 1. Variante 1 del "Virus de la policía".

Fuente: http://www.zonavirus.com/articulos/articulo-sobre-historia-del-virus-de-la-policia.asparticulo-sobre-historia-del-virus-de-la-policia.asp

[14] Aunque el acceso a las imágenes ajenas podría calificarse dentro de los delitos de los artículos 197 CP y siguientes, como ya analizábamos, lo cierto es que la conexión a internet y la retransmisión que el usuario hace –recordemos, de forma voluntaria- puede darnos a entender que realmente el sujeto activo del delito no tiene la intención de cometer el mismo. Es decir, si la cámara de seguridad tiene la opción de retransmitir de forma libre lo que está sucediendo en el hogar de su propietario, y el mismo, por omisión o desconocimiento comienza la retransmisión, entendemos que no cabe imputar al sujeto pasivo la responsabilidad por la visualización de los contenidos, en la medida en que el mismo desconoce si la retransmisión se realizó de forma consciente o involuntaria.

[15] El virus de la policía, propagado a lo largo de 2014 a lo largo de la geografía española, supuso que los ordenadores infectados mostrasen una pantalla advirtiendo del uso ilícito que se había hecho descargando material ilícito o accediendo a webs pornográficas. Dicho mensaje estaba en realidad propagado por diversos *hackers* que, haciéndose pasar por los propios cuerpos policiales, causaban en los individuos temor a consecuencias penales y procedían al pago que los *hackers* solicitaban.

[16] La *bitcoin wallet* –en castellano *cartera bitcoin*- es un tipo de monedero digital que permite recibir, enviar y contener la criptomoneda *bitcoin.*

Ilustracion 2. Variante 2 del "Virus de la policía".

Fuente: https://www.confilegal.com/20160228-la-audiencia-nacional-juzga-a-los-creadores-del-llamado-virus-de-la-policia

Con los dos ejemplos anteriores –el del sujeto cuya cámara retransmite de forma involuntaria su vida privada, y el de aquel cuyo ordenador se vio afectado por *el virus de la policía*-, queremos mostrar que realmente el acaecimiento de un *delito informático*, relacionado o no con los delitos contra la intimidad suele tener origen en la falta de conocimiento de los sujetos en el ámbito de la seguridad informática, puesto que en ocasiones el sujeto activo –el criminal que lleva a cabo el hecho antijurídico calificable como delito- actúa con conocimiento del escaso entendimiento de seguridad informática del usuario medio, buscando sacar provecho de tal desconocimiento.

No creemos que el conocimiento del *cibercriminal* sea mucho más amplio que el del titular del bien jurídico protegido, pero si nos atrevemos a afirmar que la causa de dicha ofensa ilícita penal no es otra que la falta de pericia informática del sujeto activo ocasionada por el lento desarrollo formativo y docente que la informática ha recibido en nuestro país, pues entendemos que la rápida implantación en que se ha visto plasmada la sociedad de la información no es acorde a los conocimientos que el usuario medio tiene de esta misma materia. Aunque parece que nos estemos excediendo de nuestro campo de estudio, nos atrevemos aquí a hacer una petición al legislador educativo: no entendemos que el conjunto social pueda progresar si no es mediante la inclusión en el campo docente de asignaturas destinadas a la enseñanza de la informática y la electrónica, así como, de forma especial, de la *ciberseguridad.*

El *cibercrimen* se ve así plasmado en el *ciberespionaje*, en la medida en que la finalidad de los programas informáticos ilícitos suele ser, en la mayor parte de ocasiones, la de hacer seguimiento de la actividad del sujeto cuyos bienes y derechos se han visto afectados, para conseguir sacar del mismo algún tipo de provecho o beneficio económico (directo o indirecto[17]).

[17] Aunque en ocasiones el fin del *ciberespionaje* es obtener información mediante la intromisión ilegítima, podemos afirmar con certeza que la finalidad de dicha intromisión no es otra que la de obtener un beneficio económico de cualquier tipo, aunque el mismo no se plasme de forma indirecta.

Tenemos que hacer así referencia al concepto de *spyware*, que es, al final, el elemento fundamental y clave del ciberespionaje. Si decíamos que el espionaje era la actividad por la que se obtenían de forma ilícita datos de cualquier tipo de un tercero, y sabemos que dicha actividad se lleva a cabo -en el lenguaje clásico- a través de un *espía*, dicha sujeto se plasma en el campo de la informática, en el concepto del *ciberespía*. El ciberespía aparece, a su vez, en forma de software. Recordemos que, si el *hardware* lo forman los componentes físicos de un equipo informático, el *software* está constituido así mismo por los programas que hacen funcionar a dicho equipo de hardware.

El software que comete el espionaje en el medio digital es, así, un software dedicado a extraer información del sujeto sin que el mismo sea consciente de dicha intromisión, tal y como se hace en el concepto clásico de espionaje. El *spyware* se instala así en un *segundo plano* del sistema operativo, llevando a cabo sus labores de recogida de información sin que el sujeto sea consciente de lo que está ocurriendo, siendo la única forma de conocerlo tener instalado un programa antivirus que sea capaz de hacer un análisis de la salud del sistema y detectar el funcionamiento anormal del sistema operativo ocasionado por el software espía.

Realmente, se puede decir que los conceptos de *ciberespionaje, cibercrimen o ciberataque* se diluyen en la medida en que están íntegramente relacionados, y son en muchas ocasiones resultado de un mismo grupo de operaciones, lo que conlleva al final a la dificultad de incluir un acto antijurídico informático dentro de uno de tales conceptos de forma concreta, sin que se pueda decir que también forma parte total o parcialmente de los otros. No cabe así distinción entre el cibercrimen y el ciberespionaje, dificultad de distinción que a su vez se ve plasmada en la lucha para contrarrestarlos. Si sus fronteras son difusas, también lo son aquellas dedicadas a contrarrestarlos (Puime Maroto, 2009).

Deja así paso el campo del *ciberespionaje* al ámbito de la *ciberseguridad*. Si la seguridad en el campo del derecho supone la capacidad del sujeto de enfrentarse a las lesiones de su bien jurídico protegido, haciendo uso de la regulación y de los medios que el propio ordenamiento proporciona, la ciberseguridad supone la capacidad de enfrentarse al *cibercrimen* a través de los medios que posibiliten su lucha. Creemos firmemente que la ciberseguridad se plasma así mismo en dos vertientes *(elaboración propia*):

- La defensa del bien jurídico protegido a través de los medios que la legislación estatal, autonómica y en su caso comunitaria proporcionan.

Nos referimos así a la capacidad que tiene el sujeto de defender el bien jurídico del que es titular haciendo uso de los medios que el propio derecho y su regulación proporcionan, como si de cualquier otro tipo de delito penal físico se tratare.

- La defensa del bien jurídico protegido a través de todo tipo de herramientas e instrumentos digitales o cuyo medio es digital.

En este sentido, los programas de protección antivirus o los *cortafuegos* del propio sistema operativo, que son capaces de parar las conductas antijurídicas, se consolidarían como herramientas o instrumentos digitales que son capaces de frenar la conducta antijurídica por la estructura de funcionamiento que el propio software contiene.

Si en el plano físico nos encontramos con la posibilidad de que empresas seguridad privada complementen a los Cuerpos y Fuerzas de Seguridad del Estado en el desempeño de sus funciones de salvaguarda del interés particular[18], es posible de forma análoga que la defensa de la integridad del sujeto que hace uso de sistemas informáticos sea protegida por empresas terceras, que en última instancia se encuentran plasmadas en los programas de seguridad informática como consecuencia del desarrollo de los planes y sistemas de ciberseguridad que la propia empresa ha venido desarrollando.

No obstante, y aunque para nosotros no queda duda de que la defensa del bien jurídico del sujeto pasivo del potencial delito recae en gran parte sobre la empresa privada y los programas que la misma desarrolla, creemos también firmemente que dicha defensa se hace siempre de forma adicional y complementaria a la labor que desempeñan los medios de defensa oficiales, ya sean legislativos, jurisprudenciales, o basados en los Cuerpos y Fuerzas de Seguridad del Estado, por lo que no cabe – en la medida en que nos encontramos encuadrados en un Estado Social y Democrático de Derecho cuyos valores fundamentales son la igualdad o la seguridad jurídica, entre otros- que se hable de una labor de respuesta jurídica en un ámbito que no sea el público.

Queremos por último reafirmar, concluyendo del análisis de todo lo anterior, que la ciberseguridad no debe de ser medio principal para asegurar el ciberespacio, en cuanto la misma ha de verse siempre complementada con estructuras de seguridad física que permitan actuar sobre el origen físico de toda intromisión ilegítima en la que incurra un delito informático, pues sabemos del presente estudio que todo delito informático tiene, en realidad, un origen físico directo o indirecto.

6. CONCLUSIONES

Si al inicio del trabajo nos proponíamos definir la regulación que en nuestro ordenamiento penal se ha hecho a los *delitos informáticos*, podemos concluir que dicho estudio ha sido fructífero en la medida en que el legislador ha recogido a lo largo del artículo 197 y siguientes nuevos subtipos agravados de los ya históricos delitos de descubrimiento y revelación de secretos. Dichos subtipos agravados se encuentran en armonía con los nuevos tipos básicos creados (siendo ejemplo de esta creación el delito de acceso sin autorización al sistema de información o el delito de interceptación no autorizada de transmisiones no públicas de delitos informáticos, ambos del artículo 197 bis CP).

Podemos concluir y afirmar que la labor del legislador no ha sido la de crear un delito informático, sino la de añadir a delitos ya existentes la conducta por la cual, realizando u omitiendo hechos de naturaleza antijurídica, dicha acción u omisión se realice de forma electrónica, creando así subtipos de delito que se cometen en su vertiente digital. Aunque nos hayamos referido así en nuestras páginas al delito informático o *ciberdelito*, en realidad lo que hemos hecho es un estudio de las nuevas figuras que el legislador ha creado en torno a los ya existentes *delitos relativos a la propiedad intelectual e industrial o el campo de los delitos contra la intimidad, el derecho a la propia imagen y a la inviolabilidad del domicilio.*

[18] Véase, para el desarrollo complementario de este tema, la Ley 5/2014, de 4 de abril, de Seguridad Privada.

Si decimos que el campo de aplicación del delito informático se extiende en distintos artículos y bajo Títulos distintos, lo cierto es que hemos centrado nuestra labor y hecho referencia *a los delitos contra la intimidad,* en concreto en lo que se refiere a la inclusión del subtipo de delito digital dentro del ya existente artículo 197 y siguientes del Código Penal.

Hemos definido también las principales características de la vertiente digital introducida en los citados delitos, si bien la extensión de dicho análisis ha sido proporcional a la extensión del presente trabajo, teniendo en cuenta que, más que la pormenorización de cada una de las características concretas del tipo penal – que entendemos, ya han sido suficientemente analizados por la doctrina en lo que a los elementos de los delitos contra la intimidad se refiere-, subyace realmente la importancia del estudio de la nueva vertiente digital y electrónica de este tipo de delitos.

Por último, y quizás el punto que creemos que es más actual y del que subyace la mayor labor de creación doctrinal por nuestra parte, es en lo que se refiere a los elementos de *ciberespionaje y ciberseguridad.* Hemos entendido así el ciberespionaje como una figura difusa y que posee amplias características comunes con el cibercrimen, figura que en la realidad jurídica plantea intromisiones ilegitimas en lo que a programas de *spyware* se refiere.

Decíamos que el *spyware* es el equivalente al espía físico del estudio tradicional, y que dicho espionaje ha de ser combatido, en el mundo tecnológico, mediante la ciberseguridad. Concluíamos así el trabajo con la comprensión de la *ciberseguridad* en sus dos vertientes: la que se refiere a la defensa del bien jurídico protegido por nuestro ordenamiento jurídico y legal, así como por parte de los cuerpos y fuerzas policiales, y la que se refiere, en segundo lugar, a la creación y desarrollo de sistemas de seguridad informáticos por parte de empresas de seguridad informáticas privadas (sistemas antivirus, programas cortafuegos, etc.).

Concluir también del presente trabajo la gran labor que se ha llevado a cabo por parte del legislador español a través del proceso de creación y ampliación de los delitos preexistentes, adaptando el ordenamiento jurídico existente a la llegada de nuevas situaciones que hasta ahora no estaban cubiertas ni previstas por la regulación existente en el Código Penal de 1995.

7. VALORACIÓN PERSONAL

Desde el momento en el que me embarqué en el análisis del tema –previo a la redacción del trabajo- hasta la redacción de la última de las conclusiones, puedo decir que mi interés en el tema aquí estudiado ha sido creciente, pudiendo afirmar que mi interés en el mismo se ha visto incrementado positivamente de forma exponencial.

La bibliografía consultada a través de libros y revistas en formato físico como a través de diversas fuentes de datos jurídicas de la red, me ha permitido profundizar en el estudio penal de uno de los elementos que entendemos va a cobrar mayor relevancia en nuestro ordenamiento jurídico penal a lo largo de los próximos años, dada la frecuencia con que este tipo de delitos se comete, que entendemos será cada vez superior por el

desarrollo de las nuevas tecnologías y la celeridad del avance de la sociedad de la información.

Redactar cada una de las presentes páginas me ha permitido profundizar en el estudio de un delito que, dado lo infrecuente de su estudio y la novedad de su última reforma, no habría llegado a conocer si no hubiere sido por la realización del presente trabajo.

Reafirmar mi agrado en la realización del trabajo, y no tanto en la finalización del mismo, en cuanto estoy seguro de que quedan aún muchos campos de este estudio que podrán ser profundizados en los próximos años, con la llegada de nuevas reformas por parte del legislador. Dejo aquí mi aporte y agradezco a todos los autores que han aportado, de uno u otro modo, información y fundamentación doctrinal que se ha visto plasmada, al final, en la construcción de la presente obra.

8. BIBLIOGRAFÍA

- ACURIO DEL PINO, S. (2008). *"Delitos informáticos: Generalidades"*. Profesor de Derecho Informático de la PUCE. Disponible en http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

- AIGE MUT, Mª. B. (2014). *"Los documentos electrónicos en el ámbito del proceso"*. Tesis Doctoral. Departamento de Derecho Privado, Universidad de las Islas Baleares. Disponible en: http://ibdigital.uib.es/greenstone/collect/tesisUIB/index/assoc/Aige_Mut.dir/Aige_Mut_MariaBelen.pdf

- ASOCIACIÓN DE INTERNAUTAS (2008). *"El vigilante vigilado"*. Informe extraído de https://www.internautas.org/pdf/5171.pdf

- BARREIRO, J.A (2016). *"El delito de descubrimiento y revelación de secretos en el Código Penal de 1995. Un análisis del artículo 197 del CP"*. Universidad Autónoma de Madrid. Disponible en https://revistas.uam.es/revistajuridica/article/viewFile/6240/6703

- BETRÁN PARDO, M. (2015). *"Los contenidos de WhatsApp como medio probatorio en el ámbito de las diligencias urgentes por delitos de violencia contra la mujer. Cuestiones en torno a su impugnación y a la práctica de la prueba pericial a la que se refiere la STS 300/2015, de 19 de mayo"*. Revista Pensamiento Penal. Disponible en http://www.pensamientopenal.com.ar/system/files/2015/10/doctrina4224 6.pdf

- CASABONA, R. (2006). *"El cibercrimen: nuevos retos jurídico penales, nuevas respuestas político –criminales.* Granada. Editorial Comares.

- DAVARA, M.A. (2004). *"Factbook del Comercio Electrónico"*. Navarra. Editorial Aranzadi.

- DE SOLA QUINTERO (2016). *"Delitos informáticos"*. De Sola Pate & Brown Abogados. Disponible en: https://www.desolapate.com/publicaciones/DELITOS%20INFORMATICOS_RDeSola.pdf

- ESTÉVEZ MARTÍN, S. (2010). *"Delitos Informáticos. Tipos de Delitos Informáticos. Legislación"*. Apuntes realizados para la docencia en la Universidad Complutense de Madrid. Disponible en: http://gpd.sip.ucm.es/sonia/docencia/master1011/delito.pdf

- FERNÁNDEZ-DELGADO, O. (2009). *"El descubrimiento y revelación de secretos documentales y de las telecomunicaciones. Estudio del artículo 197.1 del Código Penal"*. Madrid: Editorial Dykinson.

- FISCALÍA GENERAL DEL ESTADO (2017). *"Circular 3/2017, sobre la reforma del código penal operada por la LO 1/2015 de 30 de marzo en relación con los delitos de descubrimiento y revelación de secretos y los delitos de daños informáticos"*. Disponible en https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Circular_3-2017.pdf?idFile=5b2dd5f5-5a18-4732-bc75-7e5a63a9075c

- GARCÍA DE LA CRUZ, J. M (2009). *"Delitos informáticos"*. Madrid: Editorial El Cid Editor.

- GALLEGO YUSTE, A. (2012). *"Delitos informáticos: malware, fraudes y estafas a través de la red y cómo prevenirlos"*. Proyecto Fin de Carrera. Leganés: Universidad Carlos III de Madrid. Disponible en https://e-archivo.uc3m.es/bitstream/handle/10016/16868/pfc_alberto_gallego_yuste.pdf?sequence=1

- GONZÁLEZ COLLANTES (2015). *"Los delitos contra la intimidad tras la reforma de 2015: luces y sombras"*. En Revista de Derecho Penal y Criminología, núm. 13, 2015. págs. 51-84. Disponible en http://e-spacio.uned.es/fez/eserv/bibliuned:revistaDerechoPenalyCriminologia-2015-13-7010/pag_51.pdf

- GONZÁLEZ RUS, J.J. *"Protección penal de sistemas, elementos, datos, documentos y programas informáticos"*. Revista Electrónica de Ciencia Penal y Criminología. Disponible en http://criminet.ugr.es/recpc/recpc_01-14.html

- GUDÍN RODRÍGUEZ-MAGARIÑOS (2016). *"Nuevos delitos informáticos: phising, pharming, hacking y cracking"*. Ilustre Colegio de Abogados de Madrid. Disponible en: http://web.icam.es/bucket/Faustino%20Gud%C3%ADn%20-%20Nuevos%20delitos%20inform%C3%A1ticos.pdf

- HERNÁNDEZ DÍAZ, L (2009). *"El delito informático"*. Revista Vasca Eguzkilore, nº 23, diciembre de 2009. Disponible en https://www.ehu.eus/documents/1736829/2176697/18-Hernandez.indd.pdf

- LOREDO GONZÁLEZ, J. A (2013). *"Delitos informáticos. Su clasificación y una visión general de las medidas de acción para combatirlo".* Universidad Autónoma de Nuevo León, México. Disponible en: http://eprints.uanl.mx/3536/1/Delitos_informaticos.pdf

- MARTÍNEZ ALARCÓN, B (2006). "La filosofía hacking y cracking". Universidad Autónoma del Estado de Hidalgo. Instituto de Ciencias Básicas e Ingeniería. Disponible en: https://repository.uaeh.edu.mx/bitstream/bitstream/handle/123456789/10812/La%20filosofia%20hacking%20%26%20cracking.pdf

- MITCHELL, W. (1996). "*City of bits: Space Place and the Infobahn* ". Massachusetts: Cambridge.

- NITOIU SOTO, V. (2018). *"Delito de descubrimiento y revelación de secretos".* Máster Universitario en Acceso a la Profesión de Abogado. Universidad de Alcalá. Disponible en: https://ebuah.uah.es/dspace/bitstream/handle/10017/33140/Valentina%20Nitoiu%20Soto%2c%20TFM%20Delito%20de%20descubrimiento%20y%20revelaci%C3%B3n%20de%20secretos%2c%202018%20.pdf?sequence=1&isAllowed=y

- PUIME MAROTO, J. (2009). *"El ciberespionaje y la ciberseguridad".* En CEDESEN *"La violencia del siglo XXI. Nuevas dimensiones de la guerra".* Madrid: Ministerio de Defensa Nacional. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=4549946

- QUINTERO OLIVARES, G. (2010). *"La reforma penal de 2010. Análisis y Comentarios".* Navarra: Thomson Reuters Aranzadi.

- RAYÓN BALLESTEROS, Mª. C. (2014). *"Cibercrimen: particularidades en su investigación y enjuiciamiento".* Anuario Jurídico y Económico Escurialense, XLVII. Disponible en: https://dialnet.unirioja.es/descarga/articulo/4639646.pdf

- ROIG BATALLA, A. (2011). *"Tecnología, libertad y privacidad". En la revista* COTINO HUESO, L (2011). *"Libertades de expresión e información en internet y las redes sociales: ejercicio, amenazas y garantías".* Universidad de Valencia.

- ROMEO CASABONA, C. M (2002). "La protección penal de los mensajes de correo electrónico y de otras comunicaciones de carácter personal a través de internet". En la Revista "Derecho y Conocimiento", V.2, págs. 131-137.

- RUEDA MARTÍN, M.A (2008). *"Los ataques contra los sistemas informáticos: conducta de hacking. Cuestiones político-criminales".* En la revista *Sistema Penal*, núm. 1, 2008.

- SALVADORI, I. (2011). *"Los nuevos delitos informáticos introducidos en el Código Penal español con la Ley Orgánica 5/2010. Perspectiva de derecho comparado".* Anuario de Derecho Penal y Ciencias Sociales, VOL LXIV, 2011. Disponible en:

https://www.boe.es/publicaciones/anuarios_derecho/abrir_pdf.php?id=ANU-P-2011-10022100252_ANUARIO_DE_DERECHO_PENAL_Y_CIENCIAS_PENALES_Los_nuevos_delitos_inform%E1ticos_introducidos_en_el_C%F3digo_Penal_espa%F1ol_con_la_Ley_Org%E1nica_5/2010._Perspectiva_de_derecho_comparado

- SÁNCHEZ-ESCRIBANO, Mª. I. (2017). *"Delimitación de los conceptos de acceso y apoderamiento en el delito de descubrimiento y revelación de secretos".* Revista de Estudios Penales y Criminológicos, vol. XXXVII. Universidad de las Islas Baleares. Disponible en http://www.usc.es/revistas/index.php/epc/article/view/4063

- SANCHIS CRESPO, C. (1999). *"La prueba por soportes informáticos".* Valencia: Tirant lo Blanch.

- QUINTERO OLIVARES, G. (2001). *"Internet y propiedad intelectual".* En la revista Cuadernos de derecho judicial. Ejemplar dedicado a: Internet y derecho penal.

- RIVERA PANIZO (2009). *"Los delitos informáticos".* En Boletín Criminolóxico, núm. 11. Instituto de Criminología. Universidad de Santiago de Compostela.