Los ciberdelitos o delitos informáticos

PID_00267796

Alfonso Galán Muñoz

Tiempo mínimo de dedicación recomendado: 1 hora

Universitat Oberta de Catalunya

Alfonso Galán Muñoz

Profesor titular de Derecho penal de la Universidad Pablo de Olavide, doctor en Derecho y becario Formación de Profesorado Universitario (FPU) del Ministerio de Educación, de la Fundación Alexander von Humboldt y del Servicio Alemán de Intercambio Académico (DAAD). Ha realizado numerosas estancias de investigación en las universidades alemanas de Friburgo, Múnich, Tubinga y Berlín. Es experto en criminalidad informática y económica, temas a los que ha dedicado numerosas publicaciones, tanto nacionales como internacionales. Es investigador principal y miembro de varios proyectos de investigación nacionales y autonómicos, y responsable del Grupo PAIDI SEJ-571: Grupo de Investigación sobre el Sistema Penal y Criminología (SISPECRIM). También es el director del máster de Criminología y ciencias forenses de la Universidad Pablo de Olavide.

El encargo y la creación de este recurso de aprendizaje UOC han sido coordinados por el profesor: Josep Maria Tamarit Sumalla (2019)

Primera edición: septiembre 2019

Av. Tibidabo, 39-43, 08035 Barcelona
Realización editorial: FUOC

Índice

Objetivos

Después de trabajar los materiales que componen este módulo didáctico, el estudiante podrá alcanzar los siguientes objetivos:

1. Delimitar y diferenciar los conceptos de criminalidad informática o cibercriminalidad, derecho penal informático y ciberdelitos o delitos informáticos.

2. Tener un primer acercamiento a las características reales e irreales que han tenido influencia en la regulación penal de los delitos informáticos.

3. Conocer las razones que han determinado la enorme influencia que ha tenido el derecho penal europeo y su delimitación de los delitos informáticos en el ordenamiento español.

1. Introducción: ¿criminalidad informática, derecho penal informático, ciberdelitos?

La imparable implantación de los sistemas informáticos ha supuesto una verdadera revolución en nuestras vidas. No hay una sola faceta en nuestro quehacer diario en el que las nuevas tecnologías de la información y la comunicación no tengan, a día de hoy, un papel destacado.

Trabajamos con ordenadores. Nos comunicamos por correo electrónico. Hacemos videollamadas por Internet. Controlamos nuestros saldos bancarios a través de aplicaciones instaladas en nuestros teléfonos móviles. Compramos y vendemos toda clase de bienes y servicios a golpe de clics en nuestras pantallas. Accedemos a todo tipo de contenidos de entretenimiento (películas, series, música, etc.) utilizando plataformas digitales. Incluso establecemos y mantenemos muchas de nuestras relaciones personales gracias al uso de redes sociales desarrolladas en el seno y con la ayuda de estas tecnologías.

Las posibilidades que abren los sistemas informáticos son, como se puede comprobar, enormes. Sin embargo, también tienen un reverso negativo, dado que su utilización y expansión abre la puerta a que puedan ser utilizados para cometer toda clase de abusos contra algunos de nuestros intereses más vitales.

Por ejemplo, el hecho de que utilicemos ordenadores para realizar nuestras actividades económicas puede y, de hecho, ha sido aprovechado por algunos para enriquecerse indebidamente a costa del patrimonio de otros o para ocasionarles graves perjuicios, paralizando o inutilizando los sistemas empleados en tales actividades. Nos comunicamos y desarrollamos importantes aspectos de nuestra vida privada en un entorno digital, lo que ha llevado a algunos a tratar de descubrir nuestros secretos y vulnerar nuestra intimidad interceptando tales comunicaciones o accediendo de forma subrepticia a los datos e informaciones contenidos en nuestros sistemas. El hecho de que estas tecnologías hayan permitido difundir y comunicar, de una forma hasta hace bien poco inimaginable, toda clase de obras y contenidos de propiedad intelectual, ha llevado a que no falten quienes han querido enriquecerse ilícitamente a costa del trabajo y de las inversiones que otros habían efectuado para realizarlas.

Las posibilidades de abusos mediante sistemas informáticos no solo existen, sino que, como nos ha demostrado la realidad, son múltiples y variadas. Ello ha llevado a que se haya dejado atrás, hace ya mucho tiempo, la utópica idea de que el entorno digital podía autorregularse, sin que fuese necesario que los estados interviniesen y controlasen las actividades de los ciudadanos en la red.

En el entorno digital, como en el físico, también pueden darse conflictos sociales que han de ser resueltos mediante la intervención estatal. Y algunos de esos conflictos pueden llegar a ser tan graves que incluso pueden hacer necesaria la utilización del derecho penal.

No debe sorprender, pues, que se empezase a hablar de la aparición de lo que se denominó como «**criminalidad informática**» o «**cibercriminalidad**» y de los «**delitos informáticos**» o «**ciberdelitos**».

Todos estos conceptos, con sus matices y diferencias, tratan de agrupar aquellos comportamientos desviados, realizados gracias o a través de sistemas informáticos que presentan tal nocividad social que o bien han de ser objeto de atención por parte del derecho penal, aunque todavía no hayan recibido un adecuado tratamiento por parte de dicho derecho, o bien ya constituyen delitos reconocidos por el ordenamiento jurídico, presentando una serie de características comunes que los agrupan y distinguen del resto de figuras delictivas.

En este sentido y en primer lugar, el concepto de **criminalidad informática**, o cibercriminalidad, trata de agrupar, desde una perspectiva puramente criminológica, aquellas conductas desviadas que se realizan mediante el uso de ordenadores o en entornos digitales y no físicos (en el ciberspacio), y que se considera que deberían ser objeto de atención por parte del ordenamiento jurídico penal aunque todavía no lo sean (Miró Llinares, 2012).

Mientras tanto, quienes hablan de la existencia de un derecho penal informático o de delitos informáticos realizan una selección de los delitos que están actualmente vigentes en nuestro ordenamiento atendiendo al hecho de que o bien se realizan mediante la utilización o el empleo de sistemas informáticos, o bien protegen, exclusivamente o junto con otros valores, el bien jurídico referido a la propia seguridad de tales sistemas (Rovira del Canto, 2002).

Se presentan así, a nuestro modo de ver, dos visiones diferentes, aunque complementarias, del fenómeno objeto de este material. Una primera criminológica, centrada en el análisis fáctico de las conductas lesivas realizadas mediante sistemas informáticos o en el ciberespacio, independientemente de si han sido tipificadas ya como delito o no, y otra puramente jurídica que se dedica a analizar los aspectos comunes y las peculiaridades que presentan aquellas actuaciones que ya han sido calificadas como delito por el legislador.

El presente material se centra, exclusivamente, en el estudio de esta última visión. Es decir, va a analizar y prestar atención exclusivamente al estudio jurídico de aquellas conductas que ya son consideradas como delitos por nuestro

legislador, por más que, evidentemente, en algunos casos se haga referencia a alguna concreta faceta criminológica que ayude a entender la específica configuración o la realidad práctica a la que tales figuras delictivas están referidas.

No analizaremos, por tanto, la criminalidad informática o cibernética o la cibercriminalidad, como fenómeno fáctico o social, algo que será objeto de estudio en otras asignaturas de este máster, sino los delitos que se han ido creando a lo largo del tiempo para combatir y luchar contra algunas de las manifestaciones de dicha forma de criminalidad.

Hablaremos, por tanto, de **delitos informáticos** o, como también se les ha dado en llamar, de **ciberdelitos**. No tanto de *derecho penal informático*, por cuanto dicho término podría llevarnos a pensar que nos encontramos ante una serie de delitos que definen un sector de dicha rama del ordenamiento que agrupa determinadas figuras por tener elementos técnicos configuradores comunes que los distinguen de los demás (por ejemplo, por tener un bien jurídico común), lo que, como veremos a lo largo de este material, no se da en las principales modalidades de estos delitos.

Ejemplo

Por ejemplo, poco o nada tiene que ver el valor protegido por la estafa informática del art. 248.2.a CP y el que protege el delito de acceso ilegítimo a sistemas informáticos del 197 bis 1 CP.

Ahora bien, para hablar de delitos informáticos, lo primero que hay que hacer es determinar qué delitos podrán considerarse como tales, lo que hace que tengamos previamente que definir qué será lo que fundamente que una figura delictiva pueda ser incardinable en dicho concepto. Una vez que hemos rechazado que lo que pueda determinar la inclusión en este grupo de delitos de una figura sea que esta venga a proteger un supuesto bien jurídico común a todos ellos (por ejemplo, la seguridad de los sistemas informáticos), parece que la opción que nos quedaría sería incluir en tal concepto cualquier delito que tuviese como medio u objeto del ataque que le sea propio un sistema informático. Esto es, un ordenador, un grupo de ordenadores o los programas o datos que estos contienen y utilizan.

Sin embargo, una delimitación así llevaría a que el concepto de ciberdelito quedase carente de todo sentido o utilidad, ya que prácticamente cualquier delito que podamos imaginar (desde un homicidio hasta cualquier delito contra los consumidores o la seguridad colectiva) puede efectuarse gracias al uso de sistemas informáticos.

Es por ello por lo que consideramos que solo deben tener cabida en el concepto de **ciberdelito** aquellas figuras delictivas que aludan en su propia configuración típica a la utilización o afectación de tal clase de sistemas (véase, por ejemplo, el delito de informática del art. 248.2.a CP o el daño a datos o programas informáticos del art. 264 CP) o bien, cuando menos, sean unos delitos que, pese a no hacer referencia expresa en su tipo a dichos sistemas, se suelan cometer frecuentemente mediante su empleo o utilización (por ejemplo, el delito de comunicación pública no autorizada de obras de propiedad intelectual que castiga el art. 270.1 CP).

Este será, por tanto, el criterio que guiará la selección de temas que componen este material, lo que llevará a que estudiemos, siguiendo este mismo criterio, desde los delitos relativos a la intimidad y la protección de datos personales hasta aquellos que tutelan el patrimonio o la propiedad intelectual frente a conductas realizadas, necesaria o frecuentemente, gracias al uso de sistemas informáticos.

Conviene señalar, en cualquier caso, que existen una serie de delitos, como el del *grooming* del artículo 183 ter CP o los relativos a la pornografía infantil del artículo 189 CP, que, si bien podrían tener perfecta cabida en el referido concepto y, por tanto, ser objeto de estudio en este material, no lo serán porque sus peculiaridades y especial problemática han determinado que se haya considerado más conveniente estudiarlos de forma específica y separada en otro de los módulos de este máster.

2. Mitos y realidades de los ciberdelitos

Como acabamos de ver, nos centraremos primordialmente en el estudio técnico-jurídico de algunas de las figuras que pueden ser encuadradas en el concepto de ciberdelito o de delito informático anteriormente definido.

Sin embargo, creemos que resulta conveniente hacer una breve referencia a algunos de los caracteres, tradicionalmente atribuidos tanto a estos delitos como a sus autores, que más han influido en la normativa destinada a regular este fenómeno y, por tanto, también en la regulación jurídica de las figuras que vamos a estudiar.

Algunos de ellos rozan el mito, mientras que otros tienen mucha mayor base real, por lo que han tenido una importante influencia en la regulación penal y procesal relativa a esta clase de delitos.

2.1. Mitos referidos a los delitos informáticos

Uno de los primeros y más extendidos mitos referidos a los delitos informáticos es aquel que considera que para cometer alguna de estas figuras se han de tener unos especiales conocimientos informáticos. Esto parece responder más a aquella visión casi romántica del delincuente informático difundida por muchas películas en los años ochenta, que lo presentaban como un joven inteligente e introvertido que cometía sus delitos desde el sótano de la casa donde vivía, que a la realidad. De hecho, como se ha podido comprobar, la mayor parte de los delitos de los que nos vamos a ocupar **no los realizan expertos informáticos**, sino sujetos que tienen unos conocimientos de informática realmente básicos y que simplemente se aprovechan del acceso que tienen a los sistemas para llevar a cabo sus ilícitas actividades (Galán Muñoz, 2005).

> Precisamente por ello, como tendremos ocasión de comprobar, la mayoría de los delitos informáticos pueden ser cometidos por cualquier persona, sin que haya exigencia de que la misma tenga ninguna posición ni conocimiento especial.

Otro mito muy extendido es aquel que afirma que **los delitos informáticos suelen quedar impunes**, ya que es muy difícil o casi imposible demostrar su realización, afirmándose incluso, en esta misma línea, que existe un **anonimato** tal en Internet que hace imposible rastrearlos hasta poder determinar quién los cometió.

Frente a estas dos falsas ideas, hay que señalar que, si bien es cierto que la prueba y persecución de los delitos informáticos exigen, en muchas ocasiones, de unos ciertos conocimientos técnicos especializados, lo que ha dado lugar a la creación de grupos especialmente formados en las Fuerzas y Cuerpos de Seguridad del Estado para investigarlos y perseguirlos (por ejemplo, el Grupo de Delitos Telemáticos de la Guardia Civil o la Brigada Central de Investigación Tecnológica de la Policía Nacional), su comisión está lejos de ser indetectable o indemostrable.

De hecho, la mayor parte de las conductas delictivas realizadas mediante sistemas informáticos dejan unos rastros que son rápidamente detectados por los especialistas, lo que aporta pruebas incriminatorias muy efectivas a la hora de perseguir y sancionar a quien los realiza. Por otra parte, el famoso y supuesto anonimato y la impunidad de las actividades efectuadas en la red de redes que es Internet es puesto claramente en cuestión por la creación y utilización del sistema de conservación de datos de tráfico que instauró la Ley 25/2007, de 18 de octubre, que permite rastrear el origen del que habrían procedido todas las conductas delictivas realizadas en la red.

Bien es cierto que algunos aspectos esenciales de este último sistema, procedente de la trasposición a nuestro ordenamiento de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, y por la que se modificaba la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio, han sido puestos en tela de juicio por la sentencia del Tribunal de Justicia de la Unión Europea de 21 de diciembre de 2016, relativa a dicha Directiva, que consideró que su articulado establecía una desproporcionada restricción del derecho fundamental a la vida privada de los ciudadanos. Pero también lo es que el sistema en cuestión sigue estando operativo a día de hoy y continúa permitiendo rastrear hasta su punto de origen cualquier actividad que se haya realizado en la red, aportando una información que resulta fundamental para garantizar que su ejecución no quede en la más absoluta impunidad.

Lectura recomendada

A. Galán Muñoz (2017). «Los nuevos instrumentos de prevención y lucha contra el nuevo terrorismo: malas noticias para los derechos fundamentales de los ciudadanos». En: I. Colomer Hernández (dir.); S. Oubiña Barbolla; M. A. Catalina Benavente (coords.). *Cesión de datos personales y evidencias entre procesos penales y procedimientos administrativos sancionadores o tributarios* (págs. 81-117). Cizur Menor: Aranzadi.

2.2. Algunas realidades relevantes con influencia en los delitos informáticos

Lo anterior no puede llevarnos, sin embargo, a pensar que todo lo que se dice sobre los delitos cometidos con sistemas informáticos es falso o responde a mitos implantados en la sociedad.

Así, por ejemplo y como veremos, es indudable que, pese a que los delitos informáticos, como cualquier otro delito, pueden ser investigados y sancionados sin que reine en este ámbito una total impunidad, también lo es que existe una enorme cifra oscura de delitos que no llegan a ser perseguidos ni sancionados. En muchos casos, curiosamente por la falta de interés y colaboración que presentan sus víctimas en hacerlo.

También es cierto, por otra parte, que los sistemas informáticos permiten que casi cualquier persona pueda ocasionar unas lesiones o unos perjuicios de unas proporciones y de una intensidad que hasta hace poco resultaban casi inimaginables, utilizando unos instrumentos que están prácticamente al alcance de cualquiera.

Piénsese, por ejemplo, en los daños derivados de la creación y distribución de un virus tan simple como el célebre «I love you» o los enormes perjuicios que puede ocasionar a una entidad que uno de sus empleados introduzca unos datos falsos en su sistema de pagos a proveedores, determinando así que cada mes, o incluso cada día, se le transfiera a uno de ellos una cantidad de dinero como pago de unos suministros que realmente nunca se han llegado a efectuar.

Los sistemas informáticos representan, por tanto, y de esto no cabe duda, una fuente de enormes peligros que no se puede, ni se debe, subestimar.

Sin embargo, como veremos a lo largo de este trabajo, si analizamos los delitos que se han ido creando durante estos años para luchar contra esta clase de conductas, no tendremos más remedio que reconocer que la mayor parte de ellos no exigen, para ser apreciados, la realización de tales actuaciones altamente lesivas, sino de unas que presentan un grado de ofensividad mucho más limitado y menor.

Así, por ejemplo, para apreciar el delito de daños sobre datos o programas informáticos del artículo 264 CP no se requiere que se lesionen o se puedan lesionar los datos de múltiples y numerosos sistemas informáticos, mediante la creación de virus capaces de infectarlos, sino tan solo que se dañen o inutilicen unos pocos de tales datos, siempre y cuando, eso sí, tengan valor patrimonial o económico. Para apreciar el delito de estafa informática del artículo 248.2.a CP tampoco se necesita que la manipulación informática ocasione o pueda llegar a ocasionar perjuicios enormes a sus posibles víctimas, sino que basta, para poder apreciar su ejecución en su modalidad básica, con que ocasione una defraudación superior a los 400 €.

Pese a ello, parece que el calificativo de *informático* aplicado a todos estos delitos ha ejercido una suerte de «embrujo» en el legislador que le ha llevado a considerarlos siempre como especialmente peligrosos y lesivos, por más que no lo sean en realidad.

Solo así se explica que, en muchas ocasiones, haya decidido castigar como delitos graves lesiones ocasionadas mediante sistemas informáticos que, en caso de haberse producido por otros medios, solo se habrían sancionado como delitos leves (véase infra, por ejemplo, lo comentado con respecto a la pena que el art. 264.1 CP establece para los daños informáticos no superiores a los

400 €, en comparación con la que el delito tradicional de daños del art. 263 CP prevé para los mismos). Por otra parte, también se logra comprender que en otros supuestos el legislador haya optado incluso por adelantar las barreras de intervención penal frente a dichos ataques, castigando con las mismas penas previstas para las formas consumadas de muchos de tales delitos actuaciones que no dejarían de ser sino meros actos preparatorios de su realización (véase, en tal sentido, lo establecido, por ejemplo, por el art. 270.5.c CP en relación con el tipo básico del delito contra la propiedad intelectual), decisión que, como veremos, planteará múltiples y serios problemas de proporcionalidad.

Habrá que entender, por tanto, que la posible y real existencia de conductas o abusos informáticos altamente lesivos para algunos de los bienes jurídicos más importantes ha llevado, en algunas ocasiones, a que nuestro legislador haya procedido no solo a realizar un cuestionable **adelantamiento de la intervención penal** prevista con respecto a algunos abusos realizados con sistemas informáticos que no presentaban realmente tal lesividad, sino también a que, en muchas otras ocasiones, haya optado por efectuar una **injustificable y desproporcionada intensificación de la respuesta punitiva** prevista para la comisión de tales conductas (Galán Muñoz, 2006).

Nos encontramos, por tanto, ante una característica real de algunas actuaciones delictivas informáticas que, sin embargo y de forma errónea, ha sido predicada por nuestro legislador con respecto a todas.

Diferente es el caso de la última de las características reales de los delitos informáticos a la que vamos a hacer referencia.

Resulta indudable que si algo caracteriza al mundo digital es el hecho de que en el mismo no rigen las barreras espacio-temporales propias del mundo físico. De hecho, resulta perfectamente posible, y en modo alguno infrecuente, que la actuación delictiva realizada por un sujeto en un determinado país mediante el uso de un ordenador (por ejemplo, la creación de un virus) ocasione efectos postergados en el tiempo en lugares bien distantes de donde dicha conducta se llevó a cabo inicialmente. Incluso en otro u otros países.

Se dice, por ello, que una característica propia de los delitos informáticos es la de que presentan un marcado **carácter transnacional**. Una característica esta que se ha intensificado, sin duda, de forma exponencial como consecuencia de la frecuente utilización en la comisión de delitos de esa red de redes, que no conoce de fronteras nacionales, que es Internet.

Evidentemente, el indudable carácter trasnacional de esta clase de delincuencia representa un reto insalvable para los derechos penales nacionales. En realidad, este reto solo se puede afrontar mediante el establecimiento de una fuerte cooperación entre los diferentes ordenamientos nacionales, tanto a la hora de concretar las conductas realizadas mediante el uso de sistemas informáticos que habrán de ser sancionadas penalmente, evitando así que la ausencia

de tipificación penal de una de ellas en algún país lo convierta en un «puerto seguro» desde el que poder cometerla impunemente produciendo efectos en el resto, como articulando mecanismos de investigación e intercambio de pruebas que hagan factible investigar, perseguir y procesar de forma eficaz la ejecución transnacional de tales conductas (Galán Muñoz, 2009).

Muchos han sido los esfuerzos normativos realizados en tal sentido. Entre ellos, podemos destacar el convenio del Consejo de Europa sobre ciberdelincuencia, firmado en Budapest el 23 de noviembre de 2001. Pero también, y sobre todo, la prolija normativa referida a dicha materia emitida por la Unión Europea, cuya incidencia en el tema que nos ocupa resulta incuestionable, por lo que consideramos necesario dedicarle una referencia algo más detenida.

3. Unión Europea y delitos informáticos

Resulta imposible pasar por alto el importantísimo papel que ha desempeñado la Unión Europea en el desarrollo de la normativa española referida a los delitos informáticos.

El hecho de que muchos de los países de la Unión no tengan fronteras entre sí y que muchas de las actuaciones lesivas realizadas por medios informáticos tengan una incuestionable transcendencia económica (piénsese, por ejemplo, en el abuso de datos personales o en los delitos contra la propiedad intelectual) han llevado a que esta organización supranacional se haya mostrado especialmente activa a la hora de emitir normas armonizadoras referidas a la sanción y también a la persecución de dichos delitos.

Han sido muchas las directivas y decisiones marco que han influido de forma decisiva en la creación de los delitos informáticos vigentes en nuestro país.

Ley 25/2007

Por ejemplo, la ya citada vigente Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, encuentra su origen en la cuestionable Directiva 2006/24/CE.

De hecho, la preocupación comunitaria por armonizar las regulaciones nacionales relativas a estos delitos ha quedado claramente reflejada en el hecho de que el artículo 83.1 del Tratado de funcionamiento de la Unión Europea, tras su modificación derivada de la aprobación del Tratado de Lisboa, otorgue de forma expresa competencias a la Unión para establecer «normas mínimas relativas a la definición de las infracciones penales y de las sanciones», precisamente y entre otros ámbitos delictivos, en aquel que viene referido a lo que dicho tratado denomina como «**delincuencia informática**».

La normativa comunitaria aprobada con respecto a esta delincuencia ha sido numerosa, tanto en lo que se refiere a la materia sustantiva como a las investigadora, preventiva o procesal, hasta el punto de que su incidencia en las últimas reformas penales realizadas en nuestro país es del todo innegable.

Como tendremos ocasión de comprobar, normas tales como la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información, representan el verdadero origen de algunas de las últimas reformas realizadas en nuestro Código penal, con lo que constituyen un referente fundamental y obligatorio a la hora de interpretar lo establecido en el mismo con respecto a algunos delitos, como los de daños informáticos o el de acceso ilícito a sistemas informáticos.

Caso Pupino

Sobre la obligación de los tribunales nacionales de interpretar la normativa penal nacional de forma acorde e integrada con lo establecido por las normas comunitarias en vigor, aun cuando todavía no se hayan traspuesto a nuestro ordenamiento, véase lo establecido por el Tribunal de Justicia Europeo en su sentencia de 16 de junio de 2005, referida al caso Pupino.

Pero, además, también existen muchas otras normas comunitarias que tienen una incidencia indirecta en la delimitación de otros muchos tipos delictivos, como sucederá, por ejemplo, con las Directivas 2011/77/UE y 2012/28/UE, referidas a la protección jurídica de la propiedad intelectual, o la Directiva 98/84/CE, de 20 de noviembre, relativa a la otorgada a los servicios de acceso condicional o basados en dicho acceso.

Precisamente, entre estas últimas se encuentra una que ha de jugar un papel esencial a la hora de analizar una cuestión transversal con respecto a muchos de los delitos de los que venimos hablando.

Nos referimos a la **Directiva 2000/31/CE, de 8 de junio de 2000**, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular, el comercio electrónico en el mercado interior, norma comunitaria que dio lugar a la aprobación de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico vigente en nuestro ordenamiento. Es, precisamente, en esta ley con claro ascendente europeo, donde, entre otras cosas, se establece un peculiar y cuestionado sistema de delimitación de las responsabilidades jurídicas que se podrán llegar a atribuir a los proveedores de servicios de Internet por haber contribuido mediante la prestación de sus servicios a distribuir contenidos ajenos ilícitos o nocivos en la red, algo que evidentemente, como veremos, también puede influir en las responsabilidades penales que se les podrían imputar a resultas de su actuación cuando la misma favorezca la comisión de algunos delitos (por ejemplo, los referidos a la propiedad intelectual).

Precisamente por ello consideramos necesario comenzar nuestro estudio de los delitos informáticos analizando lo establecido en dicha Ley, para poder concretar así los efectos que su articulado podrá tener sobre los referidos sujetos a la hora de poder considerarlos como responsables (autores o partícipes) de muchos de los delitos que vamos a analizar.

Bibliografía

Galán Muñoz, A. (2005). *La estafa y el fraude mediante sistemas informáticos. Análisis del artículo 248.2 CP*. Valencia: Tirant lo Blanch.

Galán Muñoz, A. (2006). «Expansión e intensificación del derecho penal de las nuevas tecnologías: un análisis crítico de las últimas reformas legislativas en materia de criminalidad informática». *Revista de Derecho y Proceso Penal* (núm. 15, págs. 13-38).

Galán Muñoz, A. (2009). «La internacionalización de la represión y la persecución de la criminalidad informática: un nuevo campo de batalla en la eterna guerra entre prevención y garantías penales». *Revista Penal* (núm. 24).

Galán Muñoz, A. (2017). «Los nuevos instrumentos de prevención y lucha contra el nuevo terrorismo: malas noticias para los derechos fundamentales de los ciudadanos». En: I. Colomer Hernández (dir.); S. Oubiña Barbolla; M. A. Catalina Benavente (coords.). *Cesión de datos personales y evidencias entre procesos penales y procedimientos administrativos sancionadores o tributarios* (págs. 81-117). Cizur Menor: Aranzadi.

Miró Llinares, F. (2012). *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid: Marcial Pons.

Rovira del Canto, E. (2002). *Delincuencia informática y fraudes informáticos*. Granada: Comares.