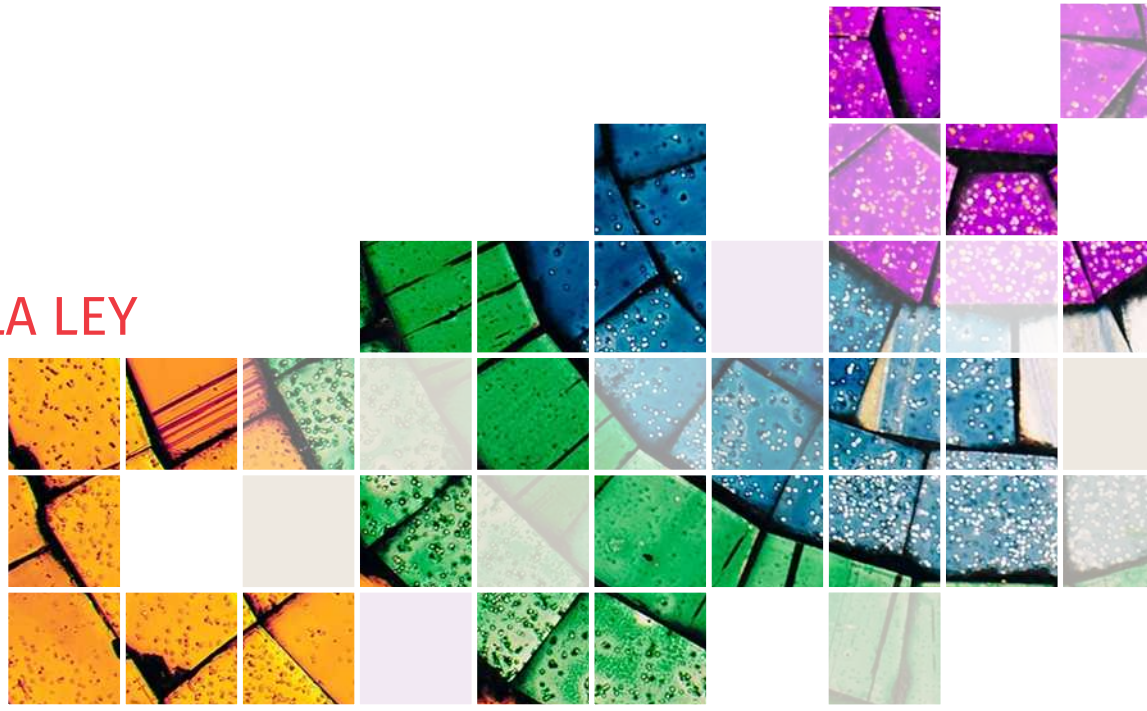
TEMAS

Delitos 2.0

Aspectos penales, procesales y de seguridad de los ciberdelitos

Moisés Barrio Andrés



LA LEY

Wolters Kluwer

TEMAS

LA LEY

Delitos 2.0

Aspectos penales, procesales y de seguridad de los ciberdelitos

Moisés Barrio Andrés

Wolters Kluwer

Wolters Kluwer
C/ Collado Mediano, 9
28231 Las Rozas (Madrid)
Tel: 902 250 500 – Fax: 902 250 502
e-mail: clientes@wolterskluwer.com
http://www.wolterskluwer.es

Primera edición: septiembre 2018

Depósito Legal: M-23756-2018
ISBN versión impresa: 978-84-9020-743-7
ISBN versión electrónica: 978-84-9020-744-4

Diseño, Preimpresión e Impresión: Wolters Kluwer España, S.A.
Printed in Spain

ciberdelitos: los que atentan contra la intimidad y privacidad y los de carácter económico. Incluso, también cabría sustantivar como ciberdelitos *strictu sensu* el intrusismo informático e interceptación de las comunicaciones (el *hacking*) y los daños informáticos y sabotajes (el *cracking*), frente a los ciberdelitos *en sentido amplio*, que afectarían a la libertad, el honor y la propia imagen, o el patrimonio entre otros bienes jurídicos más relevantes.

Nosotros no vamos a enredarnos en divagaciones sistemáticas no demasiado significantes sobre la naturaleza de las cosas, y examinaremos todos los ciberdelitos en sentido amplio atendiendo fundamentalmente a su ubicación en el Código Penal y a la frecuencia de su comisión en Internet, lo que nos lleva a analizar los siguientes:

Ciberdelito	Artículo del CP
Descubrimiento y revelación de secretos	197
Intrusismo informático e interceptación de las comunicaciones (*hacking*)	197 bis
Utilización no autorizada de imágenes previamente obtenidas con consentimiento (*revenge porn*)	197.7
Daños informáticos y sabotajes (*cracking*)	264 y ss.
Obstaculización o interrupción de un sistema informático	264 bis
Estafas	248
Abuso de sistemas informáticos (*phreaking*)	256
Calumnias	205
Injurias	208
Ciberacoso (*cyberstalking*)	172 ter
Pornografía infantil	187 y ss.
Acercamiento y embaucamiento a menores (*childgrooming*)	183 ter
Delitos contra la propiedad intelectual	270 y ss.

confidencialidad, integridad y disponibilidad de datos o sistemas informáticos; b) delitos asociados a la informática; c) delitos de contenido; y, por último, d) delitos relativos a las infracciones contra la propiedad intelectual y derechos conexos. Pero esta terminología es extraña a nuestra tradición penal.

rando el TJUE que la autoridad de control de protección de datos de un Estado miembro sí puede examinar la solicitud de una persona relativa a la protección de sus datos personales cuando éstos se hayan transferido desde un Estado miembro a un **tercer Estado que no cumpla un nivel de protección adecuado de los datos**.

1.2.2. Tipo objetivo

Debemos referirnos a los sujetos y a la conducta típica.

El **sujeto activo** puede ser, en principio, cualquiera, salvo que el agente sea la persona encargada del tratamiento o responsable de los ficheros (tipos cualificados de los arts. 197.4 o 5 CP), o una autoridad o un funcionario público quien realice la conducta típica del artículo 197.2 del Código Penal y en los términos previstos en el tipo cualificado del art. 198 CP.

El **sujeto pasivo** es el titular de los datos reservados de carácter personal o familiar registrados en archivos o ficheros, por lo que quedan excluidas las personas jurídicas (arts. 200 CP, 2.1 RGPDE y 2.1 LOPD).

En cuanto a la **conducta típica**, el precepto prevé tres modalidades típicas:

— **apoderarse**, **utilizar** o **modificar** datos reservados de carácter personal o familiar;
— **acceder** a datos reservados; y
— **alterarlos** o **utilizarlos**.

Ello requiere un comentario adicional:

a) En relación a la primera modalidad, **apoderarse** significa *hacerse con el control* de los datos (p. ej. copiarlos a una memoria USB o a Dropbox), **utilizar** comporta el *uso* de los datos, y **modificar** implica realizar alguna *alteración* en los mismos.

b) En cuanto a la segunda modalidad, **acceder** es interpretado por la doctrina precisando que no va referido a los datos, sino a los ficheros o soportes informáticos, ya que, de lo contrario, la alteración y utilización se estarían tipificando dos veces. En contra, la SAP Barcelona, Sección 6ª, de 10 de marzo de 2006 estima que el acceso se refiere a los datos y no a los ficheros, aclarando que «*no es preciso acceder a los ficheros sino que basta con el acceso a estos datos, que es lo mismo que su conocimiento, aunque se utilice otra persona para ello*».

diligencia de «peinado»)[141]. En definitiva, han de ser *sospechas fundadas*, *buenas razones y fuertes presunciones* al decir de las SSTEDH *Klass*, de 15 de junio de 1997, y *Lüdi*, de 6 de septiembre de 1998, o de las SSTS, Sala 2ª, de 22 de marzo de 2018 y de 9 de enero de 2018, y en ningún caso caben especulaciones policiales sin fundamento.

3) Principio de **idoneidad**: en atención a la utilidad de la medida, se debe definir su ámbito objetivo —teléfono, ordenador, etc.— y subjetivo —la persona o personas afectadas—, así como su duración. Es decir, para *qué*, sobre *quién* y durante *cuánto tiempo*.

4) Principio de **excepcionalidad**: sólo puede emplearse cuando no estén disponibles otras medidas menos gravosas para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho. El juez debe por tanto descartar autorizar medidas restrictivas de investigación tecnológica cuando existan otras vías menos lesivas para los derechos del investigado que, con la misma eficacia, lleven a un resultado parejo (SSTC 136/2006, 236/1999 y 171/1999).

5) Principio de **necesidad**: únicamente procederá cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero o la localización de los efectos del delito se vea *gravemente* dificultada *sin* el recurso a esta medida.

6) Principio de **proporcionalidad**: para que la medida sea considerada proporcionada a las circunstancias del caso se debe tener en cuenta la gravedad del hecho, su trascendencia social[142] o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del

(141) Hay que considerar ilegal la práctica de adoptar esta medida sin haber abierto un verdadero procedimiento penal, dentro de unas llamadas «diligencias indeterminadas» que pretenden legitimarse vulnerando el sentido y finalidad del art. 269 LECrim, pues este precepto se limita a facultar a los órganos judiciales para abstenerse de todo procedimiento cuando el hecho denunciado no revistiere caracteres de delito o la denuncia fuera manifiestamente falsa (vid. Auto de la Sala de lo Civil y Penal del TSJ de Valencia de 10 junio 1991 y Auto de la Sala 2ª del Tribunal Supremo de 18 junio 1992, caso *Naseiro*, que es el origen de esta jurisprudencia, pues realizó un completo análisis de los requisitos exigibles a fin de que las escuchas telefónicas fuesen válidas y, por tanto, aptas para servir de base de una sentencia condenatoria. Con posterioridad han sido muchas las resoluciones que se han dictado por el TS, así como por el TC, que se han remitido a la importante doctrina sentada por ese Auto de 18 de junio de 1992).

(142) La referencia que en el art. 588 bis a) LECrim se hace a la «trascendencia social del hecho» como factor de ponderación de los intereses en liza a la hora de autorizar una medida de investigación tecnológica tiene su previo origen jurisprudencial. De esta jurisprudencia cabe destacar la STS, Sala 2ª, de 23 de marzo de 2015, casando y anulando una absolución

D) Registro de la agenda del teléfono móvil

A diferencia del apartado anterior, el conocimiento de los teléfonos existentes en la agenda de un teléfono móvil no vulnera el secreto de las comunicaciones, y por ello **no es necesaria autorización judicial** para el acceso a la misma (SSTS, Sala 2ª, de 21 de noviembre de 2017 y de 17 de diciembre de 2009).

La cuestión ha quedado definitivamente zanjada en la STC 115/2013, de 9 de mayo, esclareciendo que no habiendo conversación ni manifestación de hechos por el interlocutor, no se interfirió en el ámbito propio que el secreto de las comunicaciones protege. Y la visión del número emisor que automáticamente aparece en la pantalla del receptor al margen de la voluntad de quien llama, y perceptible por cualquiera que tenga a la vista el aparato, no entraña interferencia en el ámbito privado de la comunicación; ni tampoco lo es la previa comprobación de la memoria del aparato, que tiene a tal efecto el simple carácter de una agenda electrónica y no la consideración de un teléfono en funciones de transmisión del pensamiento dentro de una relación privada de comunicación entre dos personas:

> *«No estamos, por tanto, ante un supuesto de acceso policial a funciones de un teléfono móvil que pudiesen desvelar procesos comunicativos, lo que requeriría, para garantizar el derecho al secreto de las comunicaciones (art. 18.3 CE), el consentimiento del afectado o la autorización judicial, conforme a la doctrina constitucional antes citada. El acceso policial al teléfono móvil del recurrente se limitó exclusivamente a los datos recogidos en la agenda de contactos telefónicos del terminal —entendiendo por agenda el archivo del teléfono móvil en el que consta un listado de números identificados habitualmente mediante un nombre–, por lo que debe concluirse que dichos datos "no forman parte de una comunicación actual o consumada, ni proporcionan información sobre actos concretos de comunicación pretéritos o futuros" (STC 142/2012, FJ 3), de suerte que no cabe considerar que en el presente caso la actuación de los agentes de la Policía Nacional en el ejercicio de sus funciones de investigación supusiera una injerencia en el ámbito de protección del art. 18.3CE.»*

> Distinto sería el caso si el acceso policial lo hubiera sido a cualquier otra función del teléfono móvil que pudiera desvelar procesos comunicativos (por ejemplo, acceder a las conversaciones de WhatsApp), supuesto en el que tal acceso solo resultaría constitucionalmente legítimo si media consentimiento del propio titular del terminal o autorización judicial, dada la circunstancia indubitada de que un teléfono móvil es un instrumento cuyo fin esencial es la participación en un proceso comunicativo protegido por el derecho al secreto de las comunicaciones *ex* art. 18.3 CE, como también advierte la citada STC 142/2012.

Este libro aborda la problemática de los «ciberdelitos», los *delitos 2.0*, que constituyen una nueva generación de infracciones penales que se cometen en el ámbito de Internet, mediante un estudio práctico de las características de esta forma de delincuencia, la descripción detallada de cada uno de tales delitos, y, sobre todo, de su tipificación penal, con especial atención a los últimos cambios introducidos en el Código Penal por la reforma de 2015 y a la jurisprudencia más reciente.

De este modo, se analizan en profundidad los delitos de descubrimiento y revelación de secretos, el intrusismo e interceptación de las comunicaciones (*hacking*), la protección de la intimidad, la protección de datos y el derecho a la propia imagen, la utilización no autorizada de imágenes previamente obtenidas con consentimiento en un lugar privado (*sexting* y *revenge porn*), los daños informáticos y sabotajes (*cracking*), la obstaculización o interrupción de un sistema informático, los fraudes y estafas a través de Internet, el abuso de sistemas informáticos (*phreaking*), las calumnias e injurias en la Red, el ciberacoso (*cyberstalking*), la pornografía infantil, el acercamiento y embaucamiento de menores (*childgrooming*), los delitos contra la propiedad intelectual y el ciberterrorismo.

También se examinan de forma práctica los problemas jurídico-penales de la ciberdelincuencia, el Derecho comparado, internacional y de la Unión Europea en la materia. Asimismo, la obra expone las nuevas medidas de investigación tecnológica que ha introducido la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

Finalmente, también explica los aspectos de ciberseguridad involucrados.

ISBN: 978-84-9020-743-7
9 788490 207437 3652K28424

Wolters Kluwer