uc3m | Universidad Carlos III de Madrid

OpenCourseWare

DERECHO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

Coordinadora Curso: **-Profª (PhD) María Nieves de la Serna Bilbao**

Titular de Derecho Administrativo UC3M// Departamento de Derecho Público

Co-directora del Máster Universitario en Derecho Telecomunicaciones, Protección de Datos, Audiovisual y Sociedad de la Información// Instituto Pascual Madoz

LECCIÓN 9: EL DERECHO ADMINISTRATIVO SANCIONADOR Y PENAL; TECNOLOGÍAS DE LA INFORMACIÓN

Elaborado por PhD. Fernando FONSECA FERRANDIS
Profesor Titular de Derecho Administrativo// Departamento de Derecho Público
Profesor del Máster Universitario en Derecho Telecomunicaciones, Protección de Datos, Audiovisual y Sociedad de la Información// Instituto Pascual Madoz
Universidad Carlos III de Madrid

Asignatura: Derecho de las Tecnologías de la Información
Lección 9: El Derecho Administrativo Sancionador y Penal; Tecnologías de la Información

SUMARIO:

IV. Responsabilidad penal

1. - Presentación

2.- Tipificación de los delitos relacionados con las TIC

3.- Convenio sobre ciberdelincuencia del Consejo de Europa

IV.- Responsabilidad Penal

1. Presentación

Código Penal → Se reconoce la necesidad de introducir nuevas figuras delictivas y la desaparición o modificación de aquellas figuras, ya desfasadas, que habían perdido su razón de ser.

↓

Todo acto que se vale de las TIC para su comisión

En la Exposición de Motivos del Código Penal –Ley Orgánica 10/1995, de 23 de noviembre, modificada sucesivamente- se reconoce la necesidad de tutelar valores y principios básicos de la convivencia social. De esta forma considera que cuando los valores y principios cambian las leyes también deben cambiar, y por ello corresponde al legislador introducir nuevas figuras delictivas y proceder a modificar o hacer desaparecer aquellas figuras, ya desfasadas, que han perdido su razón de ser. De acuerdo con lo anteriormente expuesto, el legislador español procedió a regular nuevos hechos que preocupan a la sociedad, y en lo que a nosotros interesa, aquellos que utilizan las Tecnologías de la Información y las comunicaciones para la realización o comisión de delitos. Sin embargo, es preciso indicar que en el Código Penal no encontramos un Capítulo o Titulo donde se recojan expresamente los delitos relacionados con las TIC. Ello no es óbice para que podamos destacar que la existencia de una reacción penal al problema, a través de todas aquellas actuaciones en las que se utilizan las TIC para la comisión de delitos.

2.- Tipificación de los delitos relacionados con las TIC

El Código penal no contiene un Título o un Capítulo específico que regule los delitos TIC. Por el contrario, a lo largo de todo Código Penal existen diversos artículos que regulan los delitos TIC.

Lo importante en este caso es que se cometan o utilicen las TIC para cometer el delito.

Los delitos relacionados con las TIC, se pueden definir con carácter general como toda actuación que se vale de las TIC para su comisión o que tiene como fin estos bienes. En toda comisión de los delitos relacionados con las TIC es necesario proceder a distinguir el **medio y el fin** por el que se cometen. Así para poder considerar que una acción es dolosa o imprudente dentro de este tipo de delitos, el **medio** por el que se cometen debe estar directamente vinculado con las TIC. Asimismo, en relación con el **fin** que se persiga con la comisión en estos delitos, es preciso indicar que el sujeto autor del ilícito, debe buscar un beneficio o tener como finalidad causar un perjuicio a otro o a un tercero. Es imposible en este trabajo tratar de analizar todos; nos limitaremos a analizar tan solo a algunos de ellos:

a) Los delitos recogidos en el Título X denominado "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en cuyo Capítulo I "Del descubrimiento y revelación de secretos". En dicho Capítulo el a**rtículo 197 CP, señala:**

1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su

consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3. El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años

…….

5. Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

6. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.

……..

b) TITULO XIII, Delitos contra el patrimonio y contra el orden socioeconómico, Capítulo II "de los Robos", cuyo **artículo 238** concreta:

" *Son reos del delito de robo con fuerza en las cosas los que ejecuten el hecho cuando concurra alguna de las circunstancias siguientes:*

4.º Uso de llaves falsas.

Artículo 239: *A los efectos del artículo anterior, junto a otros supuestos, se consideran llaves falsas las tarjetas, magnéticas o perforadas, los mandos o instrumentos de apertura a distancia y cualquier otro instrumento tecnológico de eficacia similar*

c) CAPÍTULO VI De las defraudaciones, *Sección 1.ª "De las estafas"*

Artículo 249. *1. También se consideran reos de estafa*

a) Los que, con ánimo de lucro, obstaculizando o interfiriendo indebidamente en el funcionamiento de un sistema de información o introduciendo, alterando, borrando, transmitiendo o suprimiendo indebidamente datos informáticos o valiéndose de cualquier otra manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

b) Los que, utilizando de forma fraudulenta tarjetas de crédito o débito, cheques de viaje o cualquier otro instrumento de pago material o inmaterial distinto del efectivo o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.

2. Con la misma pena prevista en el apartado anterior serán castigados:

a) Los que fabricaren, importaren, obtuvieren, poseyeren, transportaren, comerciaren o de otro modo facilitaren a terceros dispositivos, instrumentos o datos o programas informáticos, o cualquier otro medio diseñado o adaptado específicamente para la comisión de las estafas previstas en este artículo.

b) Los que, para su utilización fraudulenta, sustraigan, se apropiaren o adquieran de forma ilícita tarjetas de crédito o débito, cheques de viaje o cualquier otro instrumento de pago material o inmaterial distinto del efectivo.

d)CAPÍTULO IX. "De los daños" cuyo **artículo 264 concreta:**

1. El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese, o hiciese inaccesibles datos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave
2. El que por cualquier medio, sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, cuando el resultado producido fuera grave

e) CAPÍTULO XI De los delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores. *Sección 1.ª De los delitos relativos a la propiedad intelectual, cuyo* ***artículo* 270** señala:
1. Será castigado con la pena de prisión de seis meses a dos años y multa de 12 a 24 meses quien, con ánimo de lucro y en perjuicio de tercero, reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.
……
3. Será castigado también con la misma pena quien fabrique, importe, ponga en circulación o tenga cualquier medio específicamente destinado a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador o cualquiera de las otras obras, interpretaciones o ejecuciones en los términos previstos en el apartado 1 de este artículo.

f) *Sección 3.ª "De los delitos relativos al mercado y a los consumidores"; cuyo* **artículo 278 dispone:**

1. *El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197.*

El apartado segundo indica mayor pena si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.

3. *Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos.*

Artículo 286.

1. Será castigado el que, sin consentimiento del prestador de servicios y con fines comerciales, facilite el acceso inteligible a un servicio de radiodifusión sonora o televisiva, a servicios interactivos prestados a distancia por vía electrónica, o suministre el acceso condicional a los mismos, considerado como servicio independiente, mediante:

1.º La fabricación, importación, distribución, puesta a disposición por vía electrónica, venta, alquiler, o posesión de cualquier equipo o programa informático, no autorizado en otro Estado miembro de la Unión Europea, diseñado o adaptado para hacer posible dicho acceso.

2.º La instalación, mantenimiento o sustitución de los equipos o programas informáticos mencionados en el párrafo 1.º

2. Con idéntica pena será castigado quien, con ánimo de lucro, altere o duplique el número identificativo de equipos de telecomunicaciones, o comercialice equipos que hayan sufrido alteración fraudulenta.

g) TÍTULO XVIII, De las falsedades, CAPÍTULO II Disposiciones generales

Artículo 400.

La fabricación, recepción, obtención, tenencia, distribución, puesta a disposición o comercialización de útiles, materiales, instrumentos, sustancias, datos y programas informáticos, aparatos, elementos de seguridad o cualquier otro medio diseñado o adaptado específicamente para la comisión de los delitos descritos en los capítulos anteriores, se castigarán con la pena señalada en cada caso para los autores.

Es preciso destacar al margen de los ejemplos citados que, en algunos casos, el propio tipo no contempla específicamente el uso de las TIC, pero la realización de la acción por tales medios, sí conlleva la aplicación del tipo. Así, por ejemplo, todos aquellos casos en los que se menciona la difusión o exhibición, hechos que pueden realizarse a través de TIC. Ejemplos:

El artículo 186 impone una pena al "que, por cualquier medio directo, vendiere, difundiere o exhibiere material pornográfico" señalándose expresamente en el art.189 que *"cualquiera que sea su soporte".*

Otro ejemplo es el **artículo 578** del Código Penal que tipifica el enaltecimiento del terrorismo como delito, en los siguientes términos:

"El enaltecimiento o la justificación por cualquier medio de expresión pública o difusión de los delitos comprendidos en los artículos 571 a 577 de este Código o de quienes hayan participado en su ejecución, o la realización de actos que entrañen descrédito, menosprecio o humillación de las víctimas de los delitos terroristas o de sus familiares se castigará con la pena de prisión de uno a dos años."

La Jurisprudencia ha considerado, por ejemplo, que quien realiza enaltecimiento del terrorismo por medio del uso de las redes sociales, como Twitter, Facebook, etc., comete este delito. Así, por ejemplo, afirma la STS

65/2019, de 7 de febrero, (ECLI:ES:TS:2019:345) que *"la utilización de las redes sociales como instrumento de difusión de sus mensajes, posibilita un esparcimiento generalizado y permanente del ideario captatorio y, con ello, una mayor exposición colectiva al riesgo que el tipo penal trata de evitar".*

Al margen de la cuestión anterior, es preciso indicar que existen distintas actuaciones que están directamente relacionadas con el ámbito penal pero no se encuentran recogida en el Código Penal. Un ejemplo de ello es la regulación contenida en la Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género, que determina la obligación publicitaria de respetar la dignidad de las mujeres y el derecho a una imagen no estereotipada, ni discriminatoria, tanto en los medios de comunicación públicos como en los privados. De otro lado, se refuerza la acción de cesación o rectificación de la publicidad y con tal finalidad se legitima a las instituciones y asociaciones que trabajan a favor de la igualdad entre hombres y mujeres para su ejercicio.

Otro ejemplo es la Ley orgánica 10/2007, de 8 de octubre, reguladora de las Bases de Datos Policiales sobre identificadores obtenidos a partir del ADN que regula la creación y utilización por parte de las Fuerzas y Cuerpos de Seguridad del Estado de la información que el ADN puede ofrecer a nivel de identificación personal. La mencionada norma posibilita la inscripción en dicha base de datos de los siguientes:

a) Los datos identificativos extraídos a partir del ADN de muestras o fluidos que, en el marco de una investigación criminal, hubieran sido hallados u obtenidos a partir del análisis de las muestras biológicas del sospechoso, detenido o imputado, cuando se trate de delitos graves y, en todo caso, los que afecten a la vida, la libertad, la indemnidad o la libertad sexual, la integridad de las personas, el patrimonio siempre que fuesen realizados con fuerza en las cosas, o violencia o intimidación en las personas, así como en los casos de la delincuencia organizada, debiendo entenderse incluida, en todo caso, en el

término delincuencia organizada la recogida en el artículo 282 bis, apartado 4 de la Ley de Enjuiciamiento Criminal en relación con los delitos enumerados.

b) los patrones identificativos obtenidos en los procedimientos de identificación de restos cadavéricos o de averiguación de personas desaparecidas.

La inscripción en la base de datos policial, no precisa el consentimiento del afectado que es informado por escrito de todos los derechos que le asisten respecto a la inclusión en dicha base, quedando constancia de ello en el procedimiento. No obstante, también es posible inscribir los datos identificativos obtenidos a partir del ADN cuando el afectado hubiera prestado expresamente su consentimiento.

Los datos contenidos en la base de datos de ADN, puede ser utilizada exclusivamente por las Unidades de Policía Judicial de las Fuerzas y Cuerpos de Seguridad del Estado -Policía Nacional y Guardia Civil- y por ciertas autoridades Judiciales y Fiscales, en la investigación de los delitos. Igualmente, es posible ceder los datos contenidos en la base de datos analizada en los siguientes supuestos:

a) Cuando se trate de las Autoridades Judiciales, Fiscales o Policiales de terceros países de acuerdo con lo previsto en los convenios internacionales vigentes.

b) En el caso de las policías autonómicas para la protección de personas y bienes y para el mantenimiento de la seguridad pública o, en su caso, para la identificación de cadáveres o averiguación de personas desaparecidas.

c) También se pueden ceder al Centro Nacional de Inteligencia (CNI), que puede utilizar los datos para el cumplimiento de sus funciones relativas a la prevención de tales delitos.

3.- El Convenio sobre Ciberdelincuencia del Consejo de Europa

- Convenio de Ciberdelincuencia del Consejo de Europa firmado el 23 de noviembre del 2001 en Budapest.

Es el mayor consenso, hasta la fecha, sobre la comisión de delitos por medio de las TIC.

El Convenio de Ciberdelincuencia del Consejo de Europa -adoptado por el Comité de Ministros el 8 de noviembre de 2001, firmado en Budapest, el 23 de noviembre de 2001 y entra en vigor el 1 de julio de 2004[1]- tiene por finalidad proteger a la sociedad frente a la ciberdelincuencia. Se trata de un documento en el que existe el mayor consenso, hasta la fecha, sobre la comisión de delitos por medio de las TIC. Asimismo, persigue recoger una política penal común y adoptar una legislación que fomente la cooperación internacional en la materia. Con esta finalidad, establece el deber de adoptar las medidas legislativas -o, de cualquier otro tipo- que resulten necesarias para que el derecho interno de cada Estado miembro tipifique como delito las acciones descritas en el Convenio. En cualquier caso, resulta de gran interés dado que reflexiona sobre los profundos cambios que ha supuesto la digitalización, la convergencia y la globalización de las redes informáticas para la sociedad y la utilización de aquellas para cometer delitos o para almacenar o trasmitir por medio de dichas redes las pruebas de los delitos cometidos.
En el citado Convenio se concretan las medidas que a nivel nacional se deben adoptar y que se trata de los siguientes:

[1] El Convenio de Ciberdelincuencia fue firmado por los países participantes pero tan solo ratificado por ocho países: Albania (20-6-02), Croacia (17-10-02), Estonia (12-5-03), Hungría (4-12-03), Lituania (2-03-04), Rumania (12-5-04), Eslovenia (8-9-04) y Macedonia (15-9-04).

a) **Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos**, dentro de los cuales se incluye:

i).- El acceso ilícito, es decir, el acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático. Las Partes pueden exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención delictiva o, en relación con un sistema informático, que esté conectado a otro sistema informático.

ii).- La interceptación ilícita, es decir, la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos. Las Partes pueden exigir que el delito se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

iii).- La interferencia en los datos, la comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos.

iv).- La interferencia en el sistema, la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos.

v).- El abuso de los dispositivos, es decir, la comisión deliberada e ilegítima de los siguientes actos: a) La producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de un dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos antes mencionados; una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático; b) la posesión de alguno de los elementos mencionados con

anterioridad con el fin de que sean utilizados para cometer cualquiera de los delitos previstos antes mencionados.

b) **Delitos informáticos**, dentro de estos se incluyen:

i) La falsificación informática, es decir, cuando se cometa de forma deliberada e ilegítima, la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles.

ii) El fraude informático, los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante: a) Cualquier introducción, alteración, borrado o supresión de datos informáticos; b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona.

c) **Delitos relacionados con el contenido**, que comprende:

i) Delitos relacionados con la pornografía infantil, que comprende todo material pornográfico que contenga la representación visual de un menor comportándose de una forma sexualmente explícita; una persona que parezca un menor comportándose de una forma sexualmente explícita; e imágenes realistas que representen a un menor comportándose de una forma sexualmente explícita. Dentro de este delito se comprende la comisión deliberada e ilegítima de los siguientes actos: a) La producción de pornografía infantil con vistas a su difusión por medio de un sistema informático; b) la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático; c) la difusión o transmisión de pornografía infantil por medio de un sistema informático; d) la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona; e) la posesión de pornografía infantil en un sistema informático o en un medio. En todos estos

casos se entiende por menor toda persona menor de dieciocho años, o de un límite de edad inferior, que será como mínimo de dieciséis años.

d) **Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines,** teniendo en cuenta los siguientes extremos:

i) Las obligaciones asumidas en aplicación del Acta de París de 24 de julio de 1971 por la que se revisó el Convenio de Berna para la protección de las obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre la propiedad intelectual, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

ii) Las obligaciones que ésta haya asumido en aplicación de la Convención Internacional sobre la protección de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre las obras de los intérpretes y ejecutantes y los fonogramas, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

El Convenio también recoge otras formas de responsabilidad como corresponde a los cómplices y a las personas jurídicas. Igualmente indica que las medidas legislativas deben conducir a que los delitos, sanciones o medidas penales o no penales sean efectivas, proporcionadas y disuasorias, según los hechos cometidos.

Finalmente, hay que destacar el Convenio analizado autoriza a las Partes para adoptar medidas legislativas sobre el “Registro y confiscación de datos informáticos almacenados”, la “Obtención en tiempo real de datos informáticos” y la “Interceptación de datos sobre el contenido”.