

Tema 7. Derecho penal informático

Ética y Legislación

Medios de control social

- ▶ Informales: familia, sociedad, escuela...
- ▶ Formales: medios de control jurídico
 - ▶ Derecho Penal
 - ▶ Monopolio estatal
 - ▶ Ejercido conforme normas legales → principio de legalidad
 - ▶ ¿Principio de última ratio?
 - ▶ Derecho administrativo sancionador



Distinción entre el derecho penal y el derecho administrativo

- ▶ Por el órgano que impone la sanción
 - ▶ Administración pública
 - ▶ Órganos jurisdiccionales penales
- ▶ ¿Por la gravedad de la sanción?
 - ▶ Derecho penal: multa, penas privativas de libertad, medidas de seguridad...
 - ▶ Derecho administrativo: multa
 - ▶ Problema: gravedad de algunas multas administrativas
 - ▶ Problema: *Non bis in idem*



Derecho penal objetivo y derecho penal subjetivo

- ▶ **Derecho penal subjetivo:**
 - ▶ *ius puniendi* o derecho a castigar
- ▶ **Derecho penal objetivo:**
 - ▶ Normas. Dirigidas a:
 - ▶ Jueces
 - ▶ Ciudadanos
 - ▶ Valoraciones y principios



La pena y las medidas de seguridad como componentes del Derecho Penal

▶ Pena:

▶ Funciones:

- ▶ Retribución
- ▶ Prevención

▶ Medida de seguridad:

- ▶ Finalidad: evitar comisión de delitos
- ▶ Medidas de seguridad predelictuales/posdelictuales



Definición

► MIR PUIG:

“Conjunto de normas, valoraciones y principios jurídicos que valoran y prohíben la comisión de delitos y asocian a éstos, como presupuesto, penas y/o medidas de seguridad, como consecuencia jurídica.



La responsabilidad civil derivada de delito

- ▶ Definición
- ▶ ¿Forma parte del derecho penal?
 - ▶ Naturaleza



El derecho penal y las disciplinas del derecho penal

- ▶ La dogmática o la ciencia del derecho penal (sentido estricto)
 - ▶ Estudio del contenido interno, específicamente normativo del derecho penal
- ▶ La criminología
 - ▶ El delito como realidad
- ▶ La Política criminal
 - ▶ Conjunto de criterios empleados o a emplear en el tratamiento de la criminalidad
 - ▶ Estudio de la política criminal seguida por el Derecho Penal



Textos de referencia:

- ▶ MIR PUIG, S., *Derecho Penal. Parte General*, Ed. Reppertor, 10ª edición, 2016, 39 a 64.



CONVENIO SOBRE CIBERDELINCUENCIA

- ▶ Con el fin de definir un marco de referencia en el campo de las tecnologías y los delitos para la Unión Europea, **en Noviembre de 2001 se firmó en Budapest el “Convenio de Ciberdelincuencia del Consejo de Europa”**. En este convenio se propone una clasificación de los delitos informáticos en cuatro grupos:
- ▶ **Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:**
 - ▶ Acceso ilícito a sistemas informáticos.
 - ▶ Interceptación ilícita de datos informáticos.
 - ▶ Interferencia en el funcionamiento de un sistema informático.
 - ▶ Abuso de dispositivos que faciliten la comisión de delitos.
- ▶ Algunos ejemplos de este grupo de delitos son: el robo de identidades, la conexión a redes no autorizadas y la utilización de spyware y de keylogger.
- ▶ **Delitos informáticos:**
 - ▶ Falsificación informática mediante la introducción, borrado o supresión de datos informáticos.
 - ▶ Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.
- ▶ El borrado fraudulento de datos o la corrupción de ficheros algunos ejemplos de delitos de este tipo.



CONVENIO SOBRE CIBERDELINCUENCIA

▶ **Delitos relacionados con el contenido:**

- ▶ Producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.

▶ **Delitos relacionados con infracciones de la propiedad intelectual y derechos afines:**

- ▶ Un ejemplo de este grupo de delitos es la copia y distribución de programas informáticos, o piratería informática.



CONVENIO SOBRE CIBERDELINCUENCIA

- ▶ Con el fin de criminalizar los actos de racismo y xenofobia cometidos mediante sistemas informáticos, en **Enero de 2008 se promulgó el “Protocolo Adicional al Convenio de Ciberdelincuencia del Consejo de Europa”** que incluye, entre otros aspectos, las medidas que se deben tomar en casos de:
 - ▶ Difusión de material xenófobo o racista.
 - ▶ Insultos o amenazas con motivación racista o xenófoba.
 - ▶ Negociación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad.



DELITOS INFORMÁTICOS

- ▶ <https://delitosinformaticos.com/category/bulos-hoax>
- ▶ <https://mossos.gencat.cat/ca/temes/Internet-xarxes-socials-i-aplicacions/>
- ▶ Denuncia Guardia Civil
- ▶ <https://www.gdt.guardiacivil.es/webgdt/pinformar.php>
- ▶ Policía Nacional
- ▶ https://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html
- ▶ Comunicación hechos y consultas
- ▶ <https://www.policia.es/colabora.php>



Delito de intrusión informática

- ▶ **(Artículo 197 bis apartado primero).**
 - ▶ Se castiga el acceso o la facilitación el acceso al conjunto o parte de un sistema de información, vulnerando las medidas de seguridad y sin estar debidamente autorizado.
 - ▶ Se ha discutido mucho acerca del **bien jurídico** que se protege: mientras que parte de la doctrina se decanta por la **intimidad**, otros entienden que lo que se tutela es la **seguridad de los sistemas informáticos (opinión por la que parecen decantarse la mayoría de la doctrina)**.
 - ▶ En cuanto a la **conducta típica**, la reforma de 2015 introduce una serie de cambios, estableciendo que: *"el que por cualquier medio o procedimiento vulnerando las medidas de seguridad establecidas para impedirlo y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años"*.
 - ▶ Debemos destacar que se penará el simple acceso aunque no se haya accedido a los datos. En cuanto a las medidas de seguridad, habrá que estar al adecuado estado de la técnica, usos o costumbres.
 - ▶ Como novedad se habla expresamente de **colaboración**, por el que se facilita a un tercero el acceso al conjunto o a una parte de un sistema de información.
 - ▶ En cuanto al **sujeto activo**, aunque puede ser realizado por cualquier persona, por sus peculiaridades, en la práctica, lo normal es que sea realizado por un experto en el uso de la informática, o con conocimientos informáticos avanzados.
 - ▶ Se prevé una pena de prisión de seis meses a dos años
-



Delito de interceptación de transmisiones de datos informáticos

- ▶ (artículo 197 bis apartado segundo)
- ▶ Ésta es una figura creada ex novo tras la modificación del CP en el año 2015. El legislador ha querido criminalizar la interceptación de transmisiones no públicas de datos informáticos.
- ▶ Establece el precepto que ***"el que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde ,hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses"***.
- ▶ El **bien jurídico protegido**, es la **seguridad de los sistemas informáticos**.
- ▶ A diferencia del primer supuesto del artículo 197 bis apartado primero, éste último **se ciñe exclusivamente a la transmisión de datos informáticos**.



Delito de interceptación de transmisiones de datos informáticos

- ▶ **-Producción o facilitación a terceros para la realización de los delitos anteriores.**
- ▶ **El artículo 197 ter** castiga las conductas relacionadas con la **producción o facilitación a terceros de instrumentos para la realización de los delitos previsto en los dos apartados** primeros del artículo 197.
- ▶ *"será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 bis :*
 - ▶ *a.- un programa informático, concebido o adaptado principalmente para cometer dichos delitos*
 - ▶ *b.-una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información".*
- ▶ **.- subtipo agravado: actuar en el seno de una organización criminal**
- ▶ **El artículo 197 quater**, establece un supuesto de agravación pro actuar **en el seno de una organización o grupo criminal.**
- ▶ *"si los hechos descritos en este Capítulo se hubieran cometido **en el seno de una organización grupo criminal**, se aplicarán respectivamente las penas superiores en grado".*
- ▶ **OJO:** los alumnos advierten que determinados programas de ciberseguridad pueden ser utilizados que en principio son para proteger pueden ser utilizados torticeramente para atacar sistemas y vulnerar medidas de seguridad.



Delito de interceptación de transmisiones de datos informáticos

- ▶ *** Responsabilidad de la persona jurídica**

El **artículo 197 quinquies**, recoge el supuesto de **responsabilidad penal de la persona jurídica** *"cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en los artículos 197, 197 bis y 197 ter, se le impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el artículo 66 bis , los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b a g) del apartado 7 del artículo 33"*

- ▶ *** Responsabilidad del funcionario público**

- ▶ El **artículo 198** recoge el supuesto de responsabilidad del funcionario público, que *"fuera de los casos permitidos por la ley, sin mediar causa pro delito y prevaliéndose de sus cargo, realiza cualquiera de los delitos contra la intimidad o contra la seguridad de los sistemas informáticos".*

- ▶ *** Perseguibilidad: previa denuncia del agraviado**

- ▶ El **artículo 201** establece que **para proceder por los delitos de intrusismo informático, será precisa la denuncia de la persona afectada o de su representante legal**, de ser ésta menor de edad o discapacitada, en estos casos, podrá también denunciar el Ministerio Fiscal, denuncia que no será necesaria si los hechos se atribuyen a un funcionario público de acuerdo con lo dispuesto en el artículo 198 del CP ni tampoco cuando el delito afecte a los intereses generales o a una pluralidad de personas.
-



Delitos informáticos relacionados con la propiedad intelectual e industrial

- ▶ **Artículos 270 y ss CP**
- ▶ Con la intención de proteger la **propiedad intelectual e industrial** y preservarla de los ataques informáticos, el legislador ha querido blindarla y reforzar la seguridad de la misma frente a cualquier conducta que pueda lesionarla "**cualquiera que sea el medio y el soporte**" a través del cual se cometa la conducta delictiva.
- ▶ Se castiga no sólo la **reproducción, el plagio , la distribución, la comunicación pública o cualesquiera otras prácticas de obras literarias, artísticas o científicas**, sin la autorización de los titulares de tales derechos, sino también la facilitación del acceso a esos contenidos mediante links o enlaces de descarga con fines lucrativos, así como la **fabricación, distribución, producción , importación, almacenamiento, ofrecimiento, comercialización y cualesquiera otras prácticas similares** de productos que incorporen algún signo distintivo idéntico al original.



Delitos informáticos relacionados con la propiedad intelectual e industrial

► Señala el **artículo 270 CP** que :

" Será castigado con la pena de prisión de seis meses a cuatro años, y multa de doce a veinticuatro meses, el que , con ánimo de obtener un beneficio económico directo o indirecto y en perjuicio de tercero, reproduzca, plagie, distribuya, comunique públicamente o de cualquier otro modo explote económicamente, en todo o en parte, una obra o prestación 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.2. La misma pena se impondrá a quien , en la prestación de servicios de la sociedad de la información, con ánimo de obtener un beneficio económico directo o indirecto, y en perjuicio de tercero, facilite de modo activo y no neutral y sin limitarse a un tratamiento meramente técnico, el acceso o la localización en internet de obras o prestaciones objeto de propiedad intelectual sin la autorización de los titulares de los correspondientes derechos o de sus cesionarios, en particular, ofreciendo listados ordenados y clasificados de enlaces a las obras y contenidos referidos anteriormente, aunque dichos enlaces hubieran sido facilitados inicialmente por los destinatarios de sus servicios".



Otro tipo de delitos informáticos

- ▶ Aunque dispersos en el articulado del CP y sin una ordenación sistemática común y homogénea, encontramos "**otros delitos informáticos**", algunos de los cuales no son más que subtipos o submodalidades de delitos ya existentes (como las amenazas, injurias, calumnias) cuya comisión se produce valiéndose de las TICs; mientras que en otros supuestos estamos ante nuevos tipos penales. Sin ánimo exhaustivo o de numerus clausus, podemos citar entre ellos:



Otro tipo de delitos informáticos

- ▶ .-amenazas (**artículo 169 y ss del CP**) realizadas o difundidas a través de cualquier medio de comunicación.
 - ▶ .-calumnias e injurias (**artículo 205 y ss CP**) realizadas o difundidas a través de cualquier medio de comunicación.
 - ▶ .-fraudes informáticos (**artículo 248 del CP**)
 - ▶ .-sabotaje informático (**artículo 263 del CP**)
 - ▶ .-inducción a la prostitución de menores (**artículo 187**)
 - ▶ .-producción, venta, distribución, exhibición o posesión de material pornográfico en cuya elaboración hayan intervenido o sido utilizados menores de edad o incapaces (**artículo 189 CP**)
 - ▶ .-posesión de software informático destinado a cometer delitos (197 ter)
 - ▶ .-cualesquiera otros delitos de descubrimiento o revelación de secretos que puedan incardinarse en los artículo 197 y ss
-



Derecho penal de las TIC

- ▶ *Los llamados delitos informáticos y su positivación por parte del legislador no responde más que a la adaptación del Derecho a las necesidades reales de la sociedad. Es, sin duda, el resultado natural de una nueva realidad social fruto de la cultura TIC y que es fiel reflejo de la nueva sociedad tecnológica imperante derivada de la sinergia entre Derecho y Nuevas Tecnologías.*
- ▶ **Nuevos interrogantes y desafíos jurídicos** presenta esta simbiosis, que nos plantea en el horizonte una nueva rama del Derecho y que hará replantearnos toda la configuración clásica que hasta ahora teníamos del Derecho.
*El "**Derecho TIC**" o "**Derecho & Nuevas Tecnologías**" supondrá el futuro de una nueva disciplina científica objeto de análisis para los juristas y con ella toda una nueva especie de **ciberdelitos**: los llamados "**delitos informáticos**".*
- ▶ **Miriam Guardiola** <<http://www.legaltoday.com/practica-juridica/penal/penal/los-nuevos-delitos-informaticos-tras-la-reforma-del-codigo-penal>>

