UNIDAD DIDÁCTICA 11

MEDIDAS PROCESALES CONTRA TIPOS PENALES DE DELITOS TELEMÁTICOS

Autor: Departamento de Ciencias Jurídicas

Fecha: 28-10-2024

OBJETIVOS ESPECÍFICOS

- Conocer algunas de las cuestiones procesales relativas a delitos telemáticos e informáticos.
- Conocer la clasificación de los delitos telemáticos.
- Determinar la responsabilidad de las personas jurídicas.
- Conocer el marco jurídico de los Delitos de terrorismo.

CONTENIDOS

¿QUÉ SABE DEL TEMA?

- ¿Conoce la diferencia entre Delito Informático y el Delito contra la Informática?
- ¿Conoce los delitos no informáticos cometidos mediante medios informáticos?
- ¿Sabría determinar la responsabilidad de las personas jurídicas?

ÍNDICE DE CONTENIDOS

1.- MEDIDAS PROCESALES CONTRA TIPOS PENALES DE DELITOS TELEMÁTICOS.

En la actualidad, se considera el concepto de Delito Informático tanto el delito tradicional cometido a través de ordenador o Internet (v. gr.: injurias a través de correo electrónico) como el Delito contra la Informática, que es la acción de atacar los datos o sistemas informáticos o las vías telemáticas de comunicación, especialmente a través de Internet (v. gr. daños informáticos causados mediante un virus).

Otra clasificación de este tipo de delitos, atendiendo al Código Penal contempla la comisión de delitos comunes, pero en su modalidad informática, cometida por medios distintos de los informáticos, junto a otros delitos que atentan directamente contra los equipos informáticos o la seguridad de los datos informáticos.

1.1.- Estafa informática.

El actual **art. 249** CP precisa “1. También se consideran reos de estafa y serán castigados con la pena de prisión de seis meses a tres años:

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.

3. Se impondrá la pena en su mitad inferior a los que, para su utilización fraudulenta y sabiendo que fueron obtenidos ilícitamente, posean, adquieran, transfieran, distribuyan o pongan a disposición de terceros tarjetas de crédito o débito, cheques de viaje o cualesquiera otros instrumentos de pago materiales o inmateriales distintos del efectivo".

1.2.- Daño informático.

El artículo 264 castiga con pena de prisión de 6 meses a 3 años al que, por cualquier medio, sin autorización y de manera grave, borre, dañe, deteriore, altere, suprima o haga inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave.

El artículo 264 bis continúa castigando con igual pena de 6 meses a 3 años al que, sin estar autorizado y de manera grave, obstaculice o interrumpa el funcionamiento de un sistema informático ajeno en alguna de las formas detalladas en el propio artículo: las conductas mencionadas en el artículo anterior, introduciendo o transmitiendo datos, o destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica.

Asimismo, el artículo 264 ter prevé un castigo de prisión de 6 meses a 2 años o multa de 3 a 18 meses para quien, 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 de los dos artículos anteriores:

- Un programa informático, concebido y adaptado principalmente para cometer alguno de los delitos a que se refieren los dos artículos anteriores.
- Una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a todo o parte de un sistema de información.

El artículo 264 quater cierra este apartado extendiendo la responsabilidad criminal a las personas jurídicas que realicen las conductas descritas.

1.3.- Defraudación.

Se contempla en el artículo 255, y prevé la comisión del delito de defraudación utilizando energía eléctrica, gas, agua, telecomunicaciones u otro elemento, energía o fluido ajenos. También en el artículo 256, a quien haga uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, causando a este un perjuicio económico igual o superior a 400 euros (menor pena si el perjuicio fuera de menos valor).

1.4.- Ataque a la intimidad personal.

Se recogen fundamentalmente en el artículo 197.2 los ataques a la intimidad por medios informáticos, castigando a quien, en perjuicio de tercero, y sin su autorización, se apodere de datos reservados de carácter personal o familiar registrados en ficheros o soportes informáticos, electrónicos o telemáticos. También a quien, sin autorización, acceda por cualquier medio a los mismos o los altere o utilice en perjuicio de su titular o de un tercero.

Se contemplan otras conductas como la difusión de los datos o hechos descubiertos o la cesión a terceros, así como una agravación en caso de datos especialmente sensibles, siendo estos los relativos a la ideología, religión, salud, origen racial, vida sexual, etc. del perjudicado.

El artículo 197 bis castiga a quien, 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 a todo o parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo. También a quien, 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.

El artículo 197 ter castiga a quienes, sin autorización, y con la intención de facilitar la comisión de los delitos de los dos artículos anteriores, produzcan, adquieran para su uso, importen o faciliten a terceros:

- Un programa informático, concebido o adaptado para cometer los delitos.
- Una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a todo o parte de un sistema de información.

1.5.- Otros delitos informáticos.

No se trata de delitos informáticos propiamente dichos, pero se prevé en la normativa penal que se puedan cometer usando medios informáticos, suponiendo en la mayoría de casos una agravación de las penas por la mayor gravedad de la difusión pública y el perjuicio que esto supone. Evidentemente, no se trata de un “numerus clausus” sino que a medida que avanzan las nuevas tecnologías, aparecerán nuevos comportamientos y acciones que se trasladarán al ámbito penal. Ejemplo de ello son delitos que se pueden cometer mediante la intervención de internet o medios informáticos:

- **Delitos de Odio**. Fomentar, promover o incitar al odio o discriminación contra un grupo o persona por motivos ideológicos, racistas, de nacionalidad, de género, etc., también se prevé su comisión utilizando medios de difusión informáticos (artículo 510.3).

- **Delitos Sexuales**. Los delitos sexuales que se cometan utilizando las tecnologías informáticas así como el contacto sexual con menores a través de Internet (artículo 183) o "child grooming", o la difusión o distribución pública a través de Internet u otras tecnologías informáticas destinada a promover, fomentar o incitar la comisión de delitos de contenido sexual (artículo 189 bis).

- **Acoso**. También se prevé, cuando la acción es contactar por medios de comunicación o informáticos, o mediante la utilización de la imagen del acosado para realizar anuncios o abrir perfiles falsos en redes sociales u otros medios de difusión pública (artículo 172 ter).

- **Amenazas:** Utilizando medios informáticos, lo que supone la aplicación de las penas en su mitad superior (artículo 169.1.º).

- **Apología del Terrorismo**. Supone una agravación cuando el delito de enaltecimiento o justificación pública del terrorismo se lleve a cabo mediante difusión en Internet (artículo 578).

- **Injurias y Calumnias**. Agravación de la pena en caso de injurias graves así como de calumnias si se hacen con publicidad, lo que incluye la difusión por Internet (artículo 209).

- **Delitos contra la propiedad intelectual**. Contemplándose todas las conductas que consistan en la difusión, distribución, explotación económica o de cualquier otro modo de obras intelectuales ajenas valiéndose de medios informáticos.

1.6.- Cuestiones procesales

Pese a la heterogénea variedad de delitos que hemos visto se recogen bajo la denominación de Informáticos, existe una serie de características comunes o especificidades propias en su investigación que los singulariza de la que se realiza respecto de otros y que pueden enumerarse en las siguientes características desde el punto de vista procesal:

a) La universalidad:

Otra característica propia de los delitos informáticos es que generalmente traspasan las barreras geográficas de las realidades estatales e internacionalizan, o en el caso de Internet, universalizan, sus consecuencias.

Ello obliga a tener en cuenta ciertas reglas propias del Derecho Procesal Penal Internacional, de entre las que las más importantes afectan a la competencia, pues podría darse la posibilidad del castigo por lo mismo en más de un ordenamiento jurídico distinto ("bis in idem"). Ello no supone, que mientras ello se dilucida, los Juzgados españoles no puedan investigar un delito que no haya sido enjuiciado en ningún otro país, procediendo la acumulación en fase posterior a favor del país que tenga mejor foro, por mello, primero se toman medidas investigativas y posteriormente se determina la coordinación para un único enjuiciamiento

b) Investigación inmediata:

Son delitos que prescriben con cierta rapidez, por ello se precisa puesta en marcha de una investigación urgente. La intervención del material, se tiene presuntivamente por veraz, salvo prueba en contra.

Para garantizar la contradicción, (STS 2/12/1992, 5/02/1991 y 22/04/1991) la defensa puede proponer la oportuna contra pericia, en su caso, la impugnación explícita en su escrito de calificación, lo que conllevaría examinar al perito en el plenario (STS 5/09/1991,1/03/1994 y 1/02/1995). Caso de no optar por ninguna de estas dos líneas de defensa, los informes provenientes de organismos oficiales (igual que los análisis de drogas, huellas, balística, etc.), pueden ser traídos al proceso para ser valorados por el órgano fallador como prueba documental (STS 1/03/1994 y 11/03/1994).

c) Delitos masa:

Por afectar a delitos difusos en que se suele atacar a múltiples víctimas desconocidas, ubicadas en distintos territorios de diferentes partidos judiciales, y aun de diferentes países (delitos masa).

d) La ubicuidad como teoría para determinar su competencia:

Dado el carácter itinerante de la comisión de este tipo de delitos, que afecta al territorio de diversos países y la diferente ubicación del lugar desde donde se dirige el ataque informático y el de aquel donde éste despliega su resultado, el Tribunal Supremo, ha considerado que el delito informático, de tracto mutante e itinerante, y que establece sus efectos en múltiples ubicaciones geográficas, se produce (y por lo tanto es competente) en todos y cada uno de los sitios donde se manifiestan sus efectos, lo que incluye tanto el lugar de la acción como el del resultado (acuerdo no jurisdiccional del pleno del Tribunal Supremo de fecha 3/02/2005, según el cual:" el delito se comete en todas las jurisdicciones en las que se haya realizado algún elemento del tipo). En consecuencia, el Juez de cualquiera de ellas que primero haya iniciado las actuaciones procesales, será en principio competente para la instrucción de la causa".

Si de la investigación se determina el lugar geográfico de comisión, porque se conociera el momento de la inclusión en la red de la información o comunicación origen de la causa –A TS 22/07/2002 y 19/01/2004 -(donde está el ordenador que contiene las pruebas del delito, y desde el que se ha realizado la principal acción comisiva), cabe la inhibición a favor del Juez así determinado, ahora sí, conforme al general criterio del "forum delicti comisi" (art. 14 LECrim).

e) Escasa cobertura normativa:

En nuestro país, todavía la delincuencia informática encuentra espacios de impunidad en el ámbito normativo, así como en el ámbito judicial y policial por las dificultades técnicas y de recursos.

f) Investigación restrictiva de derechos fundamentales:

Los ordenadores, que normalmente suelen estar en lugares cerrados (domicilios, empresas, Dependencias de la Administración, etc.) encierran información en forma de escritos, fotografías, filmaciones o sonidos y archivos que muchas veces desarrollan secretos y son puras manifestaciones de la vida íntima y privada por ello, sólo pueden ser ingeridas, observadas o interceptadas con mandamiento judicial, si su titular no las permite, o no concurren situaciones de flagrancia delictiva (art. 553 LECrim).

Se plantea la duda de si es necesario el mandamiento judicial en la entrada y registro que se haga en una empresa, despachos de profesionales amparados en el secreto o en dependencias de la Administración. Para resolverla, hay que tener en cuenta que la diligencia de entrada y registro en lugar cerrado cuenta con la garantía de la intervención del Juez cuando en su interior se desarrolla vida privada. Se suele entender que las empresas, al desarrollar actividades mercantiles, no son entornos lógicos de despliegue de vida íntima o familiar, por lo que en principio, para la entrada en empresas no es preciso mandamiento judicial, si bien lo aconsejable es que los funcionarios que registren acudan amparados en un mandamiento judicial basado en un auto que lo autorice e indique los delitos que se investigan y el objeto e indicios en que se fundan, ya por lo tanto dentro de una auténtica investigación judicial.

Dicho de otra forma, no es estrictamente necesario, salvo que conste el desarrollo en su interior de vida privada (lo que puede ocurrir en los despachos, zonas no abiertas al público, reservados, privados o trastiendas) pero sí aconsejable.

g) Dificultades para apreciar la autoría delictiva:

El autor actúa casi sin riesgo y a distancia, utilizando bien técnicas humanas de anonimato uso de "nicks" o apodos, delinquiendo desde cybercafés, blogs, foros, chats, etc, o técnicas propiamente dichas que la Informática enseña y que prácticamente hacen anónima su utilización, como

pueden ser los proxys, anonimizadores Web, servidores de correo Web, remailers, dialers, o técnicas de por sí delictivas como cierto tipo de malware, como los Keyloggers.

La determinación del infractor auténtico y de la autoría concreta en uso de técnicas de ingeniería social o informática anonimizadoras, y en su caso, en los supuestos de uso compartido del ordenador, se puede determinar mediante utilización de cualesquiera medios de prueba legalmente admitidos, empezando por los que aporta la propia técnica como instrumento al servicio de la investigación procesal misma. Y si no fuese posible mediante la oportuna prueba técnica pericial para la detección de las señas IP del usuario o el rastreo de las cuentas bancarias asociadas o por la documental , y el conocimiento de la clave de usuario y contraseña de cada cual pudiese ser conocida por terceros, cabe la determinación de la convicción judicial por la testifical (uso del ordenador por el inculpado en exclusiva ,utilización de apodos, seudónimos o “nicks”, etc..), confesión del inculpado e incluso por determinación indiciaria siempre que esta sea suficientemente razonada.

En la consecución probatoria es crucial el papel de las empresas de telecomunicaciones y servidoras de Internet (proveedores de servicios) que deben colaborar con la Justicia rápidamente, llegando al balance entre esta y la legítima libertad de expresión, comercio, conocimientos y comunicación.

2.- DELITOS ECONÓMICO PATRIMONIALES VINCULADOS A LA INFORMÁTICA.

Desde el punto de vista judicial, se admite una primera clasificación de los delitos informáticos desde un triple punto de vista conforme a su definición en el Código Penal español:

A) **Ciberdelincuencia económica**: siendo estos los delitos económico patrimoniales vinculados a la informática.

B) **Ciberdelincuencia intrusiva**: Atentados por medios informáticos contra la intimidad y la privacidad.

C) **Ciberterrorismo y Ciberespionaje**: Ataques por medios informáticos contra intereses supraindividuales.

La ciberdelincuencia económica, se refiere a los ataques al patrimonio ajeno que se realizan a través de la Informática, siempre para un beneficio económico, calculable de cualquier modo sobre el patrimonio de un tercero. Suponen la mayoría de los delitos informáticos que se denuncian, pudiendo determinarse varios tipos penales en nuestra normativa penal, como por ejemplo:

- Art. 238.5 CP.-Robo inutilizando sistemas de guardia criptográfica.

- Art. 249 CP.-Estafa informática, mediante ingeniería social: a través de engaño a personas (como ocurre con el phising tradicional, o las cartas nigerianas, las estafas de ONGs, timo de sorteos, ventas de segunda mano, las falsas subastas en portales de compra y venta, etc) o bien por ingeniería informática: a través de manipulación informática o artificio semejante, descartando el engaño sobre máquinas o dispositivos técnicos (como el carding y las apropiaciones económicas por manipulación informática).

- Art. 255 CP.- Defraudación de telecomunicaciones informáticas.

- Art. 256 CP.- Hurto de tiempo informático o uso no autorizado de terminales informáticos.

- Art. 264.2 CP.- Virus o Daños informáticos, cuando se produce sobre datos. cuando los daños persiguen más que un ataque a los datos, a los sistemas informáticos, nos hallaríamos ante el Sabotaje Informático, a penar conforme al delito de Estragos (art. 346 CP) o si fuera con intencionalidad terrorista, a través de tal delito (art. 571 CP).

- Art. 270.3 CP.- Contra la Propiedad Intelectual Informática, en cualquiera de sus múltiples modalidades creativas reguladas, como puede ser la protección con entidad penal de la creación y explotación anti plagio de programas de ordenador, los intercambios masivos de productos intelectuales vehiculizados a través de la Informática o Internet, etc.

- Art. 273-275 CP.- Contra la Propiedad Industrial Informática, en cualquiera de sus modalidades protegidas siempre que tengan entidad penal.

- Art. 278-280 CP.- Espionaje informático de secretos de empresa.

- Art. 282 CP.- Publicidad engañosa. Art. 283 CP (Manipulaciones en aparatos en perjuicio del consumidor) o Art. 286 CP (Contra el Mercado Informático).

- Art. 301 CP.- Blanqueo informático de capitales.

- Art. 390 CP.- Falsedad documental, cuando el soporte sea de naturaleza informática (art. 26 CP).

3.- ATENTADOS POR MEDIOS INFORMÁTICOS CONTRA LA INTIMIDAD Y LA PRIVACIDAD.

Se trata de los ataques a la privacidad que va más allá de la intimidad, puesto que incluye todas las modalidades protegidas en el art. 18 de la Constitución Española (el honor, la intimidad personal, la familiar, la propia imagen, el domicilio, el secreto de las comunicaciones, o el uso correcto de la informática). Sería la llamada **Ciberdelincuencia Intrusiva**.

No siendo mayoría de los delitos denunciados, son un número importante de los mismos y se encuentran tipificados en el Código Penal en:

- Art. 169 y 172 CP.- Amenazas y Coacciones Informáticas.

- Art. 186-189 CP.- Distribución de material pornográfico y Pornografía Infantil.

- Art. 197-200 CP.- Descubrimiento y Revelación de secretos, que es delito informático intrusivo por excelencia.

- Art. 205-216 CP.- Injurias y Calumnias Informáticas, con el art. 211 CP se precisa qué se entiende por publicidad, es decir, propagarse por medio de imprenta, radiodifusión o por cualquier otro medio de eficacia semejante (Internet).

- Art. 417, 418 y 423 CP.- Cesión no consentida de datos ajenos, a través de la infidelidad en la custodia de documentos y violación de secretos para su venta, hecha por funcionario, que la tiene funcionalmente prohibida.

4.- . ATAQUES POR MEDIOS INFORMÁTICOS CONTRA INTERESES SUPRAINDIVIDUALES.

Se trata de los ataques más graves, siendo **Ciberespionaje y Ciberterrorismo** que afectan indiscriminadamente a intereses generales de la población, con la intención de crear pánico y terror, para subvertir el sistema político o de convivencia generalmente aceptado. Las denuncias por estos tipos son las mínimas, pero dadas las características de los mismos causan más inquietud y desasosiego a nivel social. Vienen recogidas estas actividades en nuestro Código Penal en diferentes tipos penales:

- Art. 402 CP.- Usurpación de funciones públicas mediante correo electrónico.

- Art. 598 y 603 CP.- Descubrimiento y Revelación de secretos relativos a la Defensa nacional.

Por otra parte, sociológicamente, estos delitos tienen una enorme proyección de futuro, ya que, por un lado crecen desmesuradamente año a año (por ejemplo, los delitos de Pornografía a través de Internet se han multiplicado por 4 en España entre 2004 y 2005), sus autores en la mayor parte de los casos conocidos son personas jóvenes que no alcanzan la media de los 40 años , y en muchos casos ni siquiera llegan a la mayoría de edad , a ellos se incorporan altos profesionales cualificados del mundo de la ciencia y la tecnología (ingenieros, informáticos, físicos, etc) que incluso no rehúyen la delincuencia grupal organizada, y además, año a año, evolucionan en cuanto al uso de las últimas tecnologías de la comunicación y la informática de manera que obligan a quienes los combaten a tener que actualizarse constantemente.

5.- RESPONSABILIDAD DE LAS PERSONAS JURÍDICAS Y CAUSAS DE EXENCIÓN DE LA RESPONSABILIDAD.

En España la LO 5/2010 del CP introdujo la responsabilidad penal de las personas jurídicas, acabando de esta manera con su impunidad penal que se sustentaba en el hecho de que una persona jurídica no puede cometer como tal un delito, sino que lo cometen las personas físicas que por su cuenta actúan.

Tras esta reforma legal, las personas jurídicas se convierten en sujetos activos de Derecho Penal, atribuyéndoles la **autoría** de **delitos**, al margen de la responsabilidad penal de las concretas personas físicas que los cometen.

El régimen de responsabilidad penal de las personas jurídicas introducido por la LO 5/2010 ha sido a su vez modificado por la LO 1/2015, la cual ha precisado el alcance de la responsabilidad penal de las personas jurídicas con el objetivo de proporcionar respuestas ágiles a los nuevos tipos penales y a los ya existentes, y por la LO 1/2019[1], que amplía nuevamente el catálogo de delitos por los que las personas jurídicas pueden resultar penalmente responsables.

Además, la Circular 1/2016, de 22 de enero, de la Fiscalía General del Estado, sobre la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal introducida por la Ley Orgánica 1/2015, también resulta de aplicación en este contexto.

5.1.- Alcance de la responsabilidad.

El artículo 31.bis.1 dispone que las personas jurídicas son responsables penalmente de los delitos cometidos:

- En nombre o por cuenta de las mismas, y en su beneficio directo o indirecto, por sus representantes legales o por aquellos que actuando individualmente o como integrantes de un órgano de la persona jurídica, están autorizados para tomar decisiones en nombre de la persona jurídica u ostentan facultades de organización y control dentro de la misma.

- En el ejercicio de actividades sociales y por cuenta y en beneficio directo o indirecto de las mismas, por quienes, estando sometidos a la autoridad de las personas físicas mencionadas en el párrafo anterior, han podido realizar los hechos por haberse incumplido gravemente por aquéllos los deberes de supervisión, vigilancia y control de su actividad atendidas las concretas circunstancias del caso.

[1] Ley Orgánica 1/2019, de 20 de febrero, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, para transponer Directivas de la Unión Europea en los ámbitos financiero y de terrorismo, y abordar cuestiones de índole internacional.

5.2.- Circunstancias eximentes y atenuantes.

El cumplimiento eficaz de sus obligaciones en materia de prevención de delitos puede eximir a la persona jurídica de responsabilidad penal, además de las circunstancias atenuantes de la pena que el Código Penal prevé.

a) Eximentes

La reforma de 2015 regula los programas de cumplimiento normativo o *compliance guides*, denominados modelos de organización y gestión. De esta manera y, conforme a lo dispuesto en el artículo 31 bis, apartados 2 y 4 del Código Penal, las circunstancias eximentes varían dependiendo del cargo que ocupa la persona física que comete el delito dentro de la organización de la persona jurídica:

- Si el delito es cometido por los representantes, administradores y demás personas definidas en el artículo 31.bis.1.a) la persona jurídica quedará exenta de responsabilidad cuando se cumplen las siguientes condiciones:

  1.ª el órgano de administración ha adoptado y ejecutado con eficacia, antes de la comisión del delito, **modelos de organización y gestión** que incluyen las medidas de vigilancia y control idóneas para prevenir delitos de la misma naturaleza o para reducir de forma significativa el riesgo de su comisión;

  2.ª la **supervisión** del funcionamiento y del cumplimiento del modelo de prevención implantado ha sido confiada a un órgano de la persona jurídica con poderes autónomos de iniciativa y de control o que tenga encomendada legalmente la función de supervisar la eficacia de los controles internos de la persona jurídica. En las personas jurídicas de pequeñas dimensiones, las funciones de supervisión podrán ser asumidas directamente por el órgano de administración (art. 31.bis.3 CP);

  3.ª los autores individuales han cometido el delito **eludiendo fraudulentamente** los modelos de organización y de prevención y

  4.ª **no** se ha producido una **omisión o** un **ejercicio insuficiente de** sus **funciones** de supervisión, vigilancia y control por parte del órgano al que se refiere la condición 2.ª

- Si el delito fuera cometido por los empleados o subordinados (art. 31.bis.1.b), la persona jurídica quedará exenta de responsabilidad si, antes de la comisión del delito, ha adoptado y ejecutado eficazmente un modelo de organización y gestión que resulte adecuado para prevenir delitos de la naturaleza del que fue cometido o para reducir de forma significativa el riesgo de su comisión.

Los modelos de organización y gestión deberán cumplir los siguientes requisitos:

- Identificarán las actividades en cuyo ámbito puedan ser cometidos los delitos que deben ser prevenidos.
- Establecerán los protocolos o procedimientos que concreten el proceso de formación de la voluntad de la persona jurídica, de adopción de decisiones y de ejecución de las mismas con relación a aquéllos.
- Dispondrán de modelos de gestión de los recursos financieros adecuados para impedir la comisión de los delitos que deben ser prevenidos.
- Impondrán la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención.
- Establecerán un sistema disciplinario que sancione adecuadamente el incumplimiento de las medidas que establezca el modelo.
- Realizarán una verificación periódica del modelo y de su eventual modificación cuando se pongan de manifiesto infracciones relevantes de sus disposiciones, o cuando se produzcan cambios en la organización, en la estructura de control o en la actividad desarrollada que los hagan necesarios.

b) Atenuantes.

Si la persona jurídica solo puede demostrar alguno de los sistemas de control establecidos y no todos (acreditación parcial de las circunstancias eximentes), se tendrá en cuenta para aplicar una atenuación de la pena. Sólo podrán considerarse circunstancias atenuantes de la responsabilidad penal de las personas jurídicas haber realizado, con posterioridad a la comisión del delito y a través de sus representantes legales, las siguientes actividades:

- Haber procedido, antes de conocer que el procedimiento judicial se dirige contra ella, a confesar la infracción a las autoridades.
- Haber colaborado en la investigación del hecho aportando pruebas, en cualquier momento del proceso, que fueran nuevas y decisivas.
- Haber procedido en cualquier momento del procedimiento y con anterioridad al juicio oral a reparar o disminuir el daño causado por el delito.
- Haber establecido, antes del comienzo del juicio oral, medidas eficaces para prevenir y descubrir los delitos que en el futuro pudieran cometerse con los medios o bajo la cobertura de la persona jurídica.

5.3.- Personas jurídicas exentas de responsabilidad.

Toda persona jurídica está sometida a responsabilidad penal, sin embargo, el art. 31 quinquies del CP se refiere a las personas jurídicas exceptuadas del régimen de responsabilidad penal:

- el Estado;
- las Administraciones Públicas;
- los Organismos Reguladores;
- las Agencias y Entidades públicas Empresariales;
- las Organizaciones Internacionales de derecho público;
- las Sociedades mercantiles públicas que ejecuten políticas públicas o presten servicios de interés económico general, a las que solamente les podrán ser impuestas las penas previstas en el artículo 33.7 a) y g), salvo que el juez o tribunal aprecie que se trata de una forma jurídica creada por sus promotores, fundadores, administradores o representantes con el propósito de eludir una eventual responsabilidad penal; y
- cualesquiera otras organizaciones que ejerzan potestades públicas de soberanía o administrativas.

Inicialmente los **partidos políticos** y **sindicatos** estaban exentos de responsabilidad penal, privilegio que fue suprimido por la LO 7/2012 de reforma del Código Penal (que modificó el artículo 31 bis.5).

6.- MARCO JURÍDICO DE LOS DELITOS DE TERRORISMO.

La LO 1/2019, de 20 de febrero modificó la Ley Orgánica 10/1995 del Código Penal, para transponer Directivas de la Unión Europea en los ámbitos financieros y de terrorismo, y abordar cuestiones de índole internacional, modificando el artículo 572, 573.1 (añadiendo el delito de falsedad documental), 575.3, suprimiendo el apartado 5 del artículo 576, e incorporando el artículo 580 bis. En este caso, con la LO 1/2019, se introduce la **falsedad documental**, como delito terrorista, el cual no se encontraba previsto en el art. 573 CP, con la finalidad de ser congruente con lo regulado en la Directiva 2017/541/UE.

Hay que mencionar también el Plan Estratégico Nacional de Lucha contra la Radicalización Violenta (PEN-LCRV) y el posterior Plan Estratégico Nacional de Prevención y Lucha Contra la Radicalización Violenta (PENCRAV) como medidas tomadas para actuar ante procesos de radicalización violenta que puedan derivar en actos terroristas y de corte Yihadista.

En virtud de la **LO 14/2022** quedan suprimidos los arts. 557 ter y 559 y se modifica en apartado 4 del art. 573 bis. Además, también se suprime el delito de sedición (arts. 544 a 549). El art. 573 CP incorpora una nueva definición del **delito de terrorismo** sustentada sobre las Decisiones Marco 2002/475/JAI y 2008/919/JAI del Consejo de la Unión Europea. En este sentido, establece que se considera delito de terrorismo la comisión de cualquier delito grave contra los bienes jurídicos que se enumeran en el apartado 1, cuando se lleve a cabo con alguna de las **finalidades** que se especifican en el mismo artículo:

- Subvertir el orden constitucional, o suprimir o desestabilizar gravemente el funcionamiento de las instituciones políticas o de las estructuras económicas o sociales del Estado, u obligar a los poderes públicos a realizar un acto o a abstenerse de hacerlo.

- Alterar gravemente la paz pública.

- Desestabilizar gravemente el funcionamiento de una organización internacional.

- Provocar un estado de terror en la población o en una parte de ella.

Con esta redacción, el legislador amplió, con respecto a los tipos derogados por la LO 2/2015, el catálogo de "**finalidades terroristas**". A esta enumeración se remiten todos los delitos tipificados como de terrorismo, convirtiéndose en el eje central y definitorio de la regulación vigente.

De esta forma, el tratamiento penal del terrorismo, pasa de girar en torno a la definición de organización o grupo terrorista y tipificación de las conductas que cometían quienes los integraban o colaboraban con ellos, a fundamentar la naturaleza terrorista de los actos en las finalidades perseguidas por quienes los cometen, dando cabida al castigo penal del terrorismo individual.

Asimismo, y siempre que se persigan las finalidades indicadas, el art. 573.2 CP obliga a incluir en este elenco de delitos de terrorismo, los delitos informáticos tipificados en los arts. 197 bis y 197 ter CP (*contra la seguridad de los sistemas informáticos*) y los comprendidos entre los arts. 264 a 264 quáter CP (*delitos de daños informáticos*). Sin aludir expresamente a los bienes jurídicos protegidos, ni a las finalidades terroristas, a modo de **cláusula general**, el art. 573.3 CP establece que tendrán la consideración de delitos de terrorismo "*el resto de los delitos tipificados en este Capítulo*". Esta afirmación redunda en la propia consideración que se deriva de la nomenclatura del propio Capítulo ("*de las organizaciones y grupos terroristas y de los delitos de terrorismo*").

El legislador toma en consideración para agravar las penas de los delitos contra las personas, el hecho de que la víctima tuviera la condición de autoridad referida en el art. 550.3 CP ("*miembro del Gobierno, de los Consejos de Gobierno de las Comunidades Autónomas, del Congreso de los Diputados, del Senado o de las Asambleas Legislativas de las Comunidades Autónomas, de las Corporaciones locales, del*

Consejo General del Poder Judicial, Magistrado del Tribunal Constitucional, juez, magistrado o miembro del Ministerio Fiscal"), miembro de las Fuerzas y Cuerpos de Seguridad, de las Fuerzas Armadas o empleados públicos que presten servicio en instituciones penitenciarias. De esta forma, dispone el art. 573.2 bis CP que las respectivas penas "*se impondrán en su mitad superior*".

La STS 354/17, de 17 de mayo, señala que el auto adoctrinamiento no se encuentra recogido entre los comportamientos recogidos por la Resolución 2178 del Consejo de Naciones Unidas y que diversas instancias Europas han encontrado dificultades para su tipificación. En este sentido, aboga por la necesaria interpretación restrictiva de estas conductas típicas para posibilitar su subsistencia, declarando que "*esta actividad de aprehensión de credos, debe tener una especial intensidad, sin que baste el mero acercamiento ideológico*". Asimismo, tras considerarlo como un delito de peligro, proclama que no basta la mera radicalización ideológica derivada del contenido de las páginas de internet examinadas o de los documentos poseídos, si no que se precisa la acreditación del elemento subjetivo, esto es, la finalidad de capacitarse para emprender alguno de los delitos de terrorismo.

El fenómeno de los **combatientes terroristas extranjeros**, esto es, quienes para integrarse o colaborar con una organización terrorista o para cometer un delito de terrorismo se desplacen a un territorio extranjero (art. 575.3 CP). Con la LO 1/2019 se elimina un elemento importante de la regulación anterior, como era la necesidad de que ese territorio estuviera controlado por un grupo u organización terrorista. Ahora, como consecuencia de la mencionada reforma, se consumará el tipo penal simplemente con el **traslado o desplazamiento a ese territorio extranjero**, con las finalidades descritas.

El legislador ha recogido incluso **formas imprudentes** de comisión del delito, como la negligente omisión de los deberes emanados de la normativa sobre blanqueo de capitales y prevención de la financiación del terrorismo (véase, la Ley 10/2010, de 28 de abril de prevención y blanqueo de capitales y de la financiación del terrorismo).

Por otro lado, prevé la posibilidad de **atenuación** de la pena en dos supuestos:

- A quienes hubieran abandonado voluntariamente sus actividades delictivas, se presentarán a las autoridades confesando los hechos en que hubiera participado y a quienes colaboren activamente con estas para impedir la producción del delito o coadyuve a la obtención de pruebas.

- A quienes fueran responsables de hechos que fueran objetivamente de menor gravedad, atendidos el medio empleado o el resultado producido.

En cuanto a la **reincidencia internacional**, en todos los delitos de terrorismo, la condena de un juez o tribunal extranjero será equiparada a las sentencias de los jueces o tribunales españoles a los efectos de aplicación de la agravante de reincidencia.

Con la modificación que tuvo lugar con la LO 1/2019 se incluyó la responsabilidad de las personas jurídicas, cuando sea responsable de acuerdo con el artículo 31, en que se le impondrán las siguientes penas:

b) Multa de dos a cinco años, o del doble al cuádruple del perjuicio causado cuando la cantidad resultante fuese más elevada, si el delito cometido por la persona física tiene prevista una pena de más de dos años de privación de libertad.

c) Multa de seis meses a dos años, o del doble al triple del perjuicio causado si la cantidad resultante fuese más elevada, en el resto de los casos.

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.

7.- ASPECTOS RELEVANTES

- Hay delitos que no son delitos informáticos propiamente dichos, pero se prevé que se puedan cometer usando medios informáticos, suponiendo en la mayoría de casos una agravación de las penas.
- Toda persona jurídica está sometida a responsabilidad penal, salvo las excepciones previstas.
- La ubicuidad se refiere a que el delito informático es de tracto mutante e itinerante, y que establece sus efectos en múltiples ubicaciones geográficas, se produce (y por lo tanto es competente) en todos y cada uno de los sitios donde se manifiestan sus efectos, lo que incluye tanto el lugar de la acción como el del resultado.

EVALUACIÓN

1.- Una de las características de los delitos informáticos es que por afectar a delitos difusos en que se suele atacar a múltiples víctimas desconocidas, ubicadas en distintos territorios de diferentes partidos judiciales, y aun de diferentes países. Por tanto, se les conoce como:

a) Delito imposible.
b) Delito difuso.
c) Delito masa.

2.- Cuando en delitos telemáticos hablamos de "Child grooming", nos referimos a:

d) Delitos de acoso.
e) Delitos sexuales.
f) Ninguna de las dos.

3.- Para apreciar la reincidencia internacional en los delitos de terrorismo, la condena de un juez o tribunal extranjero:

a) Será equiparada a las sentencias de los jueces o tribunales españoles a los efectos de aplicación de la agravante de reincidencia si se trata de países europeos.
b) Será equiparada a las sentencias de los jueces o tribunales españoles a los efectos de aplicación de la agravante de reincidencia.
c) Será equiparada a las sentencias de los jueces o tribunales españoles a los efectos de aplicación de la agravante de reincidencia previa solicitud de reconocimiento a la autoridad extranjera por reciprocidad.

SOLUCIONES

Pregunta número	Respuesta
1	c
2	b
3	b