CUESTIONES PRÁCTICAS Y PROCESALES RELACIONADAS CON LA INVESTIGACIÓN DE LOS DELITOS INFORMÁTICOS.

A. COMPETENCIA TERRITORIAL Y PERSECUCIÓN INTERNACIONAL.

1. En esta materia rige, como regla general, el **principio de ubicuidad,** sin perjuicio de que posteriormente de llegar a determinarse el lugar geográfico concreto desde el que se introdujeron los datos delictivos en la red, se acuerde la inhibición de la causa a favor del Juez así determinado, ello conforme a la regla general del fórum delicti comisi del art. 14 de la L.E.Cr.

1. En la persecución de los delitos informáticos no rige, como regla general, el principio de universalidad, salvo lo dispuesto para casos especiales por las leyes procesales y los Convenios Internacionales.

B. INTERRUPCIÓN DE LA PRESCRIPCIÓN.

En esta materia rigen las reglas generales de interrupción del art. 132-2 del CP (cuando el procedimiento se dirija contra la persona indiciariamente responsable del delito o falta), si bien con el fin de evitar la impunidad de las desconocidas personas que actúan desde detrás de la pantalla de un ordenador, bastará para ello con conocer la dirección IP desde la que se llevó a cabo la actividad delictiva.

C. OBTENCIÓN DE DATOS DE TRÁFICO.

1. Contenidos protegidos por el secreto de las comunicaciones.

a) Intervenciones telefónicas:

1.a)1 En todo caso, la entrega de los listados de llamadas telefónicas por las compañías telefónicas a la policía, sin consentimiento del titular del teléfono, requiere resolución judicial.

1.a)2 De entre todos los datos de tráfico generados en el transcurso de una comunicación telefónica, merecen la protección reforzada del art. 18.3 CE los datos indicativos del origen y del destino de la comunicación, del momento y duración de la misma y, por último, los referentes al volumen de la información transmitida y el tipo de comunicación entablada.

1.b) Intervención en relación con terminal telefónico sustraído: En estos casos cabe adoptar la medida de intervenir el teléfono asociado al IMEI.

1.c) Escucha y/o grabación directa de conversaciones: es posible realizarla, con autorización judicial, por medio de micrófonos ocultos o direccionales, siempre cumpliendo las exigencias requeridas para las intervenciones telefónicas.
No puede considerarse vulneración del secreto de las comunicaciones la escucha, sin utilización de ningún artificio, de una conversación telefónica o directa por hallarse el que las oye en las inmediaciones del lugar en que se produce.

a) **Visionado directo del número entrante:** en ningún caso no entraña interferencia en el ámbito privado de la comunicación.

b) **Hallazgos casuales:** son válidos, pero la continuidad en la investigación de un hecho delictivo nuevo requiere de una nueva autorización judicial; y si se trata de un delito conexo con el ya investigado, dictará una nueva autorización ampliada a investigar en la misma causa; si se trata de un delito totalmente autónomo e independiente del anterior el Juez deberá, dictar una expresa autorización judicial que permita la continuación de la escucha e incoar la oportuna causa aparte con el oportuno testimonio.

c) **Sistema SITEL:** Es ajustada a Derecho la utilización probatoria de las conversaciones grabadas por el sistema SITEL, no siendo necesaria, en principio, la práctica de una compleja y dilatoria prueba pericial informática para conocer o acreditar las características básicas del sistema.

2. **Revelación de datos por uno de los interlocutores:** Las grabaciones y revelaciones de las conversaciones por uno de los interlocutores no afectan al secreto de las comunicaciones, pudiendo afectar al derecho a la intimidad, de modo que, en principio, pueden admitirse como medio de prueba, sin perjuicio de su impugnación.

3. **Utilización del teléfono intervenido por terceras personas:** La autorización judicial abarca todas las comunicaciones realizadas por el teléfono intervenido, aunque lo utilicen otras personas no mencionadas en la resolución autorizante; quedando cubierta la intervención aunque la intervención se realice en base a la titularidad del terminal e incluso la utilización esporádica del teléfono por otra u otras personas del grupo de personas implicado en la actividad delictiva enjuiciada no exige una nueva autorización de la intervención en función de quien lo utilice en cada momento.

4. **Acceso a los datos internos de los teléfonos móviles:** El acceso a la libreta de contactos de un teléfono móvil no supone una injerencia en el secreto a las comunicaciones; sí lo supone en cambio el acceso a los datos de registro de llamadas y el acceso a los mensajes contenidos en el teléfono móvil de los detenidos hayan sido o no leídos; todo ello exigirá autorización judicial.

5. **Datos relativos al IMEI:** La información albergada en la serie IMSI e IMEI no puede catalogarse como dato externo integrable en el contenido del derecho al secreto de las comunicaciones.

6. **Investigación de la dirección IP:** Los rastreos policiales para localizar direcciones IP pueden realizarse sin necesidad de autorización judicial, si bien tras la averiguación del IP, las subsiguientes actuaciones de identificación y localización de quién sea la persona que tiene asignado ese IP se deben llevar a cabo bajo control judicial. Cuando la Policía necesita dirigirse a una operadora para conocer el IP utilizado debe considerarse necesario obtener autorización judicial, conforme a las previsiones de la Ley 25/2007.

7. **Acceso al corro electrónico:** Debe considerarse necesaria la autorización judicial para acceder a cualquier mensaje enviado por correo electrónico, ya se trate de correo electrónico enviado y recibido pero no leído, correo en fase de transferencia o correo ya enviado, recibido y leído y que se encuentra almacenado.

8. **Cesión de datos almacenados por las operadoras:** La Ley 25/2007, de 18 de octubre *de Conservación de Datos de Comunicaciones Electrónicas* exige autorización judicial para acceder no sólo a los datos de tráfico (terminales conectados, identificación de los usuarios y datación de la comunicación), sino también a otros que podrían ser calificados como servicios de valor añadido. La Ley 25/2007 restringe la posibilidad de cesión a la averiguación de delitos graves, si bien conforme a una exégesis teleológica y sistemática, la gravedad debe

definirse en atención a las circunstancias concretas del hecho, teniendo en cuenta el bien jurídico protegido y la relevancia social de la actividad, de conformidad con la jurisprudencia recaída en relación con los delitos susceptibles de ser investigados mediante intervenciones telefónicas.

9. **Conversaciones en chats:** Las conversaciones o comunicaciones que tengan lugar en el seno de chats o foros de Internet abiertos a cualquier usuario no pueden considerarse comprendidas dentro del ámbito del derecho fundamental al secreto de las comunicaciones, por lo que no precisan de autorización judicial para su grabación u observación; siendo necesaria, en cambio, dicha autorización cuando se use la opción de comunicación bidireccional cerrada entre dos usuarios.

10. **Acceso a contenidos y datos almacenados en discos duros:** La apertura de archivos de un disco duro o de unidades externas de un ordenador tampoco afecta al derecho al secreto de las comunicaciones. Los Cuerpos y Fuerzas de Seguridad del Estado pueden, sin autorización judicial, intervenir y reproducir un soporte magnético o electrónico (por ejemplo, la lectura de un disco duro), aun cuando su contenido material pudiera afectar al derecho a la intimidad del art. 18.1 CE si concurren razones de urgencia y se persigue un fin constitucionalmente legítimo.

D. CONVENIOS INTERNACIONALES EN LA MATERIA:

1. **El Convenio de Budapest sobre cybercrimen:** constituye una importante herramienta para la lucha contra los delitos cometidos por medios informáticos, si bien debería extenderse a otros muchos países para ser realmente eficaz.

2. **Cooperación jurídica internacional y policial:** Los Tribunales españoles no deben supervisar la legalidad de las intervenciones telefónicas practicadas en el extranjero conforme a la normativa española, cuando se trate de países en los que se mantengan de modo efectivo los mismos valores y principios que en España se consagran en la Constitución. No obstante, queda abierta la posibilidad de valorar si las intervenciones fueron practicadas conforme a las normas procesales del país de obtención, correspondiendo a quien lo alega la prueba de la inobservancia de la norma procesal extranjera y por tanto de la ilegalidad y nulidad de esta prueba. No es procedente imponer a servicios policiales extranjeros las mismas normas internas que la doctrina jurisprudencial interna ha establecido para los servicios policiales españoles.

A.- MEDIOS DE PRUEBA EN LOS DELITOS INFORMÁTICOS. ESPECIAL ESTUDIO DE LOS DELITOS DE PORNOGRAFÍA INFANTIL, CONTRA LA INTIMIDAD, REVELACIÓN DE SECRETOS, COACCIONES, AMENAZAS O INJURIAS, QUEBRANTAMIENTOS, ESTAFAS, FALSEDADES Y DAÑOS.

MEDIOS DE PRUEBA

1. Prueba electrónica, videográfica e informática

Es un medio de prueba autónomo, cuya naturaleza, para la mayoría de la doctrina y Jurisprudencia es de prueba documental, por las semejanzas que guarda el soporte electrónico con el documento y por la idoneidad de su introducción al proceso como tal. El art. 26 CP da un concepto amplio de documento en el que tiene cabida.

Como requisito de admisibilidad está sometida a **u**n previo juicio de licitud, es decir, que la prueba se haya obtenido sin violar derechos fundamentales, pues, en otro caso, sería nula (art. 11.1 LOPJ).

Su relevancia a efectos procesales está condicionada a la **a**utenticidad (no manipulación) y a la integridad (conservación del contenido).

2. Las **grabaciones como medio de prueba**, aun no reguladas en la Lecr. se ha admitido por la doctrina y jurisprudencia su validez como prueba en el proceso penal (SSTS 6-05-1993, 6-04-1994, 27-02-1996, 19-04-1996, 25-11-1996)

-Los requisitos que debe reunir para admitirse como prueba válida son:

1. Que se haya obtenido de forma lícita, sin vulnerar el derecho de privacidad de las personas, que incluye el derecho a intimidad, a la propia imagen y a la autodeterminación informativa, si no será nula (art. 11.1 LOPJ).

Se deben respetar dos límites: el locativo (no invadir la esfera domiciliaria) y funcional (en el curso de una investigación criminal) (STC 14/03).

2. Que se aporte correctamente al proceso penal. Garantías a cumplir son: control judicial de la legitimidad de la filmación, entrega inmediata del material, autenticidad e integridad.

-La utilización de videocámaras.

Sólo está regulada jurídicamente la videovigilancia policial, es decir, las cámaras utilizadas y controladas por las Fuerzas y Cuerpos de Seguridad del Estado en lugares públicos o de acceso público, que se rige por la Ley Orgánica 4/1997, de 4 de agosto (LOV), y Reglamento de desarrollo, Real Decreto 596/1999, de 16 de abril.

Se utilizan para captar y grabar imágenes y sonidos en lugares públicos, abiertos o cerrados para asegurar la convivencia ciudadana o prevenir la comisión de delitos, faltas e infracciones contra la seguridad pública.

Quedan excluidas las instaladas por las Unidades de Policía Judicial para investigar delitos y faltas y descubrir y asegurar al delincuente, en cuyo caso la aplicable será la LECR.

-La **videovigilancia no policial son l**as videocámaras utilizadas por las **empresas y personal de seguridad privada**, así como por **particulares o empresarios** (para vigilar sus domicilios o empresas).

No existe regulación específica, por lo que habrá que acudir a la LOPD.

Respecto a las que utilizan las empresas y personal de seguridad privada (Vigilantes de Seguridad, Jefes de Seguridad y escoltas privados, Guardas particulares de campo y Detectives privados) debe tenerse en cuenta la Ley 23/1992 de 30 de julio de Seguridad Privada y su Reglamento de desarrollo, Real Decreto 2364/1994, de 9 de diciembre.

-V**alor probatorio pleno de las grabaciones policiales (STS 9-05-2005, 23-07-1999).** El art. 282 LECr. autoriza a la Policía a utilizar esta diligencia de investigación, debe realizarse en el curso de una investigación criminal y fuera del domicilio.

Si el emplazamiento de aparatos de filmación o de escucha invade el espacio restringido reservado para la intimidad de las personas (domicilio o lugares privados) se necesita autorización judicial.

-V**alor probatorio de las grabaciones realizadas por particulares:** Las imágenes grabadas por un particular al presenciar un hecho delictivo en la vía pública y que son presentadas en la comisaría de Policía o en el Juzgado tienen el valor de denuncia con toda la fuerza probatoria de las imágenes, que quedan unidas como piezas de convicción, y pueden incorporarse al plenario como documental reforzada por la testifical del autor de la grabación (**STS 24-04-2006)**

-Respecto a las **imágenes captadas por los profesionales de los medios de comunicación, no hay inconveniente en su utilización como** medio probatorio, que se verá reforzado por la testifical del periodista, que revestirá plena objetividad al ser ajeno al proceso (**STS de 12-01-2011)**

-respecto la grabación obtenida por periodistas con "cámara oculta", la STC de 30 de enero de 2012 declaró ilegítima esta técnica de investigación periodística denominada "cámara oculta", por suponer una vulneración clara del derecho a la intimidad y a la propia imagen, que no se justifica por el derecho a la libertad de información.

-No deben considerarse **válidas las grabaciones subrepticias realizadas por detective privado en un ámbito privado(AAP Jaén, Sección 2ª, 17-12-2012)**

-las grabaciones realizadas por las cámaras automáticas de los bancos u otros establecimientos obligados a disponer de determinadas medidas de seguridad, tienen valor probatorio al no haber afectación de derechos fundamentales, siendo la

prueba las grabaciones

3. ¿Cómo se incorporan al proceso con plenas garantías?

Los **medios audiovisuales**: entrega del CD DVD o instrumento utilizado (también un teléfono móvil), que puede ir acompañado de transcripción escrita (ej. Mensajes en un teléfono móvil).

Los achivos informáticos: mediante su impresión en papel-Documental o por examen directo del Juez del ordenador –reconocimiento judicial.

-Correo electrónico. La intervención de los mismos (en transmisión o ya almacenados en el ordenador o en los servidores) es una valiosa fuente de información en la investigación de los delitos cometidos a través del correo (ej. contra la intimidad, injurias, daños, etc.).

Son cuestiones problemáticas la autoría o participación del emisor, la dificultad de obtener los datos de tráfico o intervenir los contenidos cuando la cuenta de correo usada pertenece a una empresa cuya sede esté en EEUU (como Hotmail, Yahoo, Gmail), y la determinación de la competencia de los Tribunales españoles. Se resuelve aplicando el criterio de la ubicuidad.

Es obligatorio investigar los hallazgos casuales de otros delitos heterogéneos que se conozcan y surjan durante la instrucción atendiendo a su flagrancia patente y la regla de conexidad de los arts. 17.5 y 300 LECr.

Respecto a la recogida y conservación (art. 334 LECr.), cuando los correos intervenidos están en el servidor y no en el ordenador, el Secretario Judicial debe abrirlos y pasarlos al disco duro, precintar éste (para evitar su borrado o manipulación), y llevárselo al Juzgado, siendo el encargado de su custodia. También puede imprimir los correos en papel, levantando diligencia de su contenido, fecha y hora, lo que servirá como documental.

¿**Cómo se introducen en el juicio oral?**

*Como una documental pública, en caso de haberse volcado los datos en un soporte legible (normalmente CD/dvd), bajo la supervisión del Secretario Judicial, no siendo necesaria la presencia del Secretario en la operación de volcado (**STS de 14 de mayo de 2008)**

*Como documental privada, si es aportada por un particular (afectado o no), en cuyo caso debe acudir a juicio como testigo a ser sometido a interrogatorio.

-SMS Y MMS de teléfonos móviles. Les es aplicable todo lo analizado respecto al correo electrónico en caso de intervención judicial.

En los casos en que la víctima acuda a la Policía o al Juzgado con el terminal, se deberá hacer una transcripción o transmisión a papel del mensaje a fin de incorporarlo al proceso. El/a Secretario/a Judicial debe realizar un cotejo de las transcripciones con el texto original y tal diligencia constituirá una prueba documental preconstituída que se valorará como tal junto con el resto de la prueba.

Si el mensaje lo aporta un tercero, sólo sería lícito si lo hace una de las partes de la conversación.

- foros, Messenger, redes sociales, chat, blogs.

Les es aplicable lo analizado respecto al correo electrónico y SMS-MMS.

- **Las webs:** la **responsabilidad civil del prestador de servicios por comentarios injuriosos alojados en sus páginas web.**

La Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y comercio electrónico (LSSICE), en su art. 16 establece que sólo serán responsables si tienen conocimiento efectivo" de dicho contenido (la jurisprudencia lo ha interpretado como conocimiento por cualquier medio faheciente, sin necesidad de previa declaración de ilicitud)y no han procedido a suprimirlo.

4. Para garantizar la autenticidad e integridad de la fuente probatoria es necesario mantener la cadena de custodia.

La STC de 29 de septiembre de 2003, en interpretación del art. **338 LECr.,** dispone los requisitos a cumplir:

1.La descripción del material ocupado en Acta o diligencia del Secretario Judicial (art. 334 LECr.), y a presencia del Secretario también igualmente al bloqueo y precinto de cualquier ranura o puerto; 2. Custodia en un lugar adecuado; 3 Constancia en la causa de la cadena de custodia; 4. Control judicial de la recogida y custodia.

La irregularidad de la cadena de custodia no constituye, de por sí, vulneración de derecho fundamental alguno, y además se exige la prueba de su manipulación efectiva.

5. Las formalidades deben cumplirse en el volcado a papel y en la realización de copia de seguridad son:

Del volcado a papel se levantará un acta o diligencia por el Secretario Judicial, en la que se reflejará las personas intervinientes, se describirá lo que se ha hecho y se firmará por todos.Debe intervenir un perito, el Secretario Judicial y el imputado, pudiendo hacerlo el Juez y el resto de partes si quieren.

En caso de realización de copia de seguridad en CD o DVD, el perito informará de las operaciones, y el Secretario Judicial describirá el dispositivo y el lugar donde queda almacenado, pudiendo las partes obtener copias.

No es necesaria la presencia del Secretario durante la operación material de volcado de datos (STS 15-11-1999), bastando con que esté al inicio y al final.

Para garantizar que coincide lo ocupado y la copia se debe hacer una prueba técnica de contraste o hash, antes y después del análisis.

6. Práctica de la prueba: en el juicio oral

-Cabe alegar como cuestión previa la posible nulidad de la intervención realizada y por tanto la legitimidad de la prueba así obtenida, que normalmente debe ser anunciada en el escrito de defensa del imputado, aunque nada obsta a que se alegue ex novo, en cualquier caso debe plantearse el debate, pues si no lo hace ya no cabrá que lo plantee en el recurso.

¿Cómo se incorporan al plenario?

--Mediante la lectura de las diligencias del sumario de imposible reproducción en juicio –art. 730 LECr. Incluye la reproducción de videos, CDS, etc.

Si las partes disponen de una copia de la grabación o de la transcripción escrita no es necesario su reproducción en juicio o al menos no de todo el contenido.Si no se impugna en todo o en parte la transcripción de las cintas, y se tiene por reproducida, no se le puede negar valor probatorio a tales transcripciones.Si no se pide ni en el juicio oral ni en la apelación la audición de las cintas no puede el querellado quejarse de indefensión.

-examen directo por el Juez (726 LECr.).

Tal prueba puede complementarse con la pericial y con la testifical en orden a acreditar que son auténticas las manifestaciones grabadas (que no han sido manipuladas) o que son veraces la imágenes de un video o de un archivo informático, o se corresponde la voz grabada con la de la persona a la que se atribuye. La prueba pericial fonométrica para la identificación de voces es una prueba que no atenta contra la intimidad ni la integridad física, pues no equivale a una prueba de confesión.

Si la parte interesada no la solicita en el momento procesal oportuno está admitiendo implícitamente la autenticidad de las voces. En todo caso, el Juez o Tribunal puede llegar a esta convicción por las pruebas testificales de los policías que realizaron los seguimientos y escuchas o por su propia percepción en juicio.

7. Pericial informática

-El Objeto de la pericia informática es el análisis de los equipos informáticos o dispositivos de almacenamiento de datos (discos duros externos, CD-DVD, memorias USB) intervenidos por la Policía y a disposición de la Autoridad Judicial

-E**s necesario mandato judicial, salvo que haya auto de entrada y registro en domicilio o vehiculo,** habilitación suficiente para examinar los ordenadores o equipos hallados.

-Se suelen realizar normalmente por **Organismos oficiales especializados**, que son el Departamento de Delitos Telemáticos de la Guardia Civil (DDT) o Brigada de Investigación Tecnológica de la Policía Judicial, y los departamentos especializados de la Policía Autonómica (Ertzaintza, Mossos D'Esquadra). Si bien debe hacerse la pericia por informáticos distintos de los que realizaron la intervención.Aunque es admisible que se designen Peritos a **técnicos informáticos de un organismo oficial perjudicado** por el delito, y también cabe nombrar como **Peritos a expertos (Ingenieros en Informática o Técnicos en Informática) para que auxilien** a la comisión judicial en las entradas y registro. Acompañan a la Policía como Peritos Judiciales. Son válidas las pericias particulares, pero plantean problemas de cadena de custodia y posible afectación de derechos fundamentales.

-Para garantizar la **contradicción** en juicio la defensa puede proponer una contrapericia o impugnar expresamente la pericial oficial, impugnación que debe hacerse en el escrito de calificación en el que debe proponerse la práctica de la pericial para el juicio oral, a fin de someter al perito al interrogatorio oportuno.

-Validez de la prueba: Garantizar la cadena de custodia sobre el objeto de la pericia y el volcado de datos en una copia de seguridad, sobre ésta trabajará el perito, conservándose el original en el Juzgado, disponible por si quieren las partes proponer una contrapericia.

-**La ausencia del Secretario Judicial en la diligencia de volcado de datos no invalida la prueba**. Ahora bien, sí es conveniente que se haga por los peritos un resumen digital o hash del disco original y otro de la copia y si coinciden eso garantiza que no ha habido manipulación.

-**Pueden estar presentes las partes durante la realización de la pericia, tanto la** acusación como la defensa pueden concurrir con su representación, debiendo solicitarlo cuando se les notifique la resolución judicial que acuerde la confección de la pericia.**Las partes pueden ejercitar su contradicción e**mitiendo observaciones durante la realización de la pericia (art. 480 LECr.), interrogando al perito al emitir sus conclusiones cuando acude a ratificar el informe al Juzgado (art. 483 LECr.) ó aportando una contrapericia.

-Puede practicarse como prueba preconstituida y como prueba anticipada, por lo que deberá estar presente el Secretario Judicial para tener plena validez probatoria.

-E**s necesaria su práctica en juicio oral,** salvo en los supuestos de prueba preconstituida o anticipada. En estos casos se aportará como documental y será evaluable en sentencia sin necesidad de ratificarse en juicio el perito, salvo que las partes la impugnen, debiendo ser traído el perito al juicio a ser sometido a contradicción (STS 27-12-2006)

-Está admitida la intervención pericial por videoconferencia (arts. 325 y 731 bis LECR.), para la emisión, ratificación y sometimiento a contradicción.

-**La falta de exhibición en juicio del material o soporte informático para examinar la información y datos sobre los que versó la pericial no priva de validez al informe pericial.**

-**Impugnación por la defensa. Tiempo y forma. Eficacia.**

Son pericias preconstituidas las actas policiales de recogida de discos duros, archivos, etc. así como las diligencias de volcado de datos.No precisan ratificación si no son impugnados materialmente, no bastando la mera impugnación formal.

Las periciales emitidas por organismos públicos son periciales documentadas con privilegio jurisprudencial consolidado, no siendo necesaria la ratificación del perito, salvo que se impugne o se solicite su presencia en juicio para someterlo a contradicción.

El resto de pericias, documentadas o no, sí deben ser ratificadas en el juicio oral.

-La valoración de la pericia informática como el resto de la prueba electrónica será conforme al art. 741 Lecr. Valoración racional conforme a las normas de la sana crítica, máximas de experiencia y conocimientos científicos aceptados.

-DELITO DE PORNOGRAFIA INFANTIL. ART. 189

***Distribución de material pornográfico (art. 189.1 b).**

-Para la investigación será necesario la ocupación del equipo o archivos informáticos, para lo cual deberá obtener la Policía autorización de entrada y registro en el domicilio del sospechoso.

-Para la obtención de la identificación IP (huella de entrada al programa) no será necesario obtener tal autorización judicial.

-Para la identificación del titular del terminal telefónico o usuario de internet sí se necesita consentimiento del interesado o autorización judicial. Así lo imponen los arts. 6 y 7 de la L*ey 25/2007, de 18 de octubre, de Conservación de Datos Relativos* a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones. Y así lo ha interpretado el Pleno de la Sala Segunda del Tribunal Supremo celebrado el 23 de febrero de 2010 acordó que el Ministerio Fiscal precisará de tal autorización para obtener de los operadores los datos conservados que se especifican en el *art. 3 de la Ley 25/2007, de 18 de octubre.*

-Facilitar la difusión:Descarga de archivos (peer to peer).

Se cumplen los requisitos objetivos del tipo con la posesión en el equipo informático de archivos de contenido pedófilo y la descarga de los mismos mediante programas de intercambio de archivos peer to peer (emule, Lphant).

El elemento subjetivo del tipo delictivo exige que el sujeto sea perfectamente conocedor del contenido ilegal de los archivos que descargaba así como de la facilitación de descarga que con ello procuraba a terceros usuarios. Basta el dolo eventual.

Esta exigencia deriva del **Acuerdo adoptado por el Pleno no jurisdiccional de esta Sala celebrado el 27 de Octubre de 2009**:"Una vez establecido el tipo objetivo del *art. 189.1 b) CP*, el subjetivo deberá ser considerado en cada caso, evitando incurrir en automatismos derivados del mero uso del programa informático empleado para descargar los archivos"(vid. También *SSTS como las de 30 de Enero* o *28 de Octubre de 2009*).

En casos de remisión de archivos pornográficos por correo electrónico se considera distribución aun cuando el destinatario no haya llegado a abrir su correo.

***Posesion material pornográfico. Art. 189.2**

-Se castiga la posesión voluntaria y con conocimiento del contenido pedófilo de los archivos. Es necesaria una tenencia prolongada que, en el caso de Internet ha de ir referida a un almacenamiento en disco duro o en otro soporte.

-No se castiga, por tanto, la descarga accidental y subsiguiente borrado ni el simple visionado de pornografía o el mero acceso al material pornográfico.

-Son pruebas fundamentales la documental que se intervenga (correos, archivos, etc.) y la pericial informática, debiéndose permitir a la defensa si lo solicita una contrapericia, facilitándole una copia de aquellos.

*La D**irectiva 2011/93/UE, de 13 de diciembre del Parlamento y del Consejo de Europa relativa a la lucha contra los abusos sexuales la explotación sexual de menores y la pornografía infantil, crea** *la necesidad de una nueva modificación del Código Penal, habiendo dado un plazo a los Estados Miembros para su cumplimiento que termina el 18 de diciembre de 2013. Entre otras novedades, s*e debe castigar la Pornografía virtual y técnica o asistencia a espectáculos porno de menores, así como introducir las técnicas de blocking y prohibir el acceso a determinadas profesiones a persona condenadas por estos delitos.

-DELITOS CONTRA LA INTIMIDAD. DESCUBRIMIENTO Y REVELACION DE SECRETOS. ART. 197 CP

El delito del apdo. 11, que recoge dos tipos básicos, es un delito de intención, en la modalidad de delito mutilado de dos actos, uno de apoderamiento, interceptación o utilización de artificios técnicos, unido a un elemento subjetivo adicional, el dolo, consistente en el ánimo de realizar un acto posterior, descubrir el secreto, o vulnerar la intimidad de otro, sin necesidad de que éste llegue a producirse.

Se consuma con el apoderamiento o interceptación, si se difunden, revelan o ceden a terceros entramos en la fase de agotamiento, lo que constituye el tipo agravado del apdo. 3º.

El apartado 5º del precepto incluye otro supuesto agravado destinado a proteger el núcleo duro del derecho a la intimidad, además de los casos en que la víctima fuere un menor de edad o un incapaz.

Se incluirían las grabaciones no consentidas de actos sexuales ó el apoderamiento de mensajes obrantes en un teléfono móvil. Ha de tenerse en cuenta que el secreto no afecta a los propios partícipes de la comunicación, sin perjuicio de que en ciertos supuestos éstos podrían llegar a vulnerar el derecho a la intimidad de su comunicante.

En el apartado 2º se castiga el acceso a bases de datos personales protegidos informáticamente. Se protegen sólo los datos reservados, pertenecientes al ámbito personal y familiar, recogidos en ficheros o bases de datos.

Se considera dato inocuo un dato administrativo al alcance de los empleados de un centro, y, por tanto, no punible, sin perjuicio de su sanción en el ámbito administrativo sancionador.

Es necesario que se actúe sin legitimación y el perjuicio a tercero o al titular de los datos.

En la Jurisprudencia encontramos casos de accesos a bases de dato médicos y bases de datos policial, cuya condena o absolución depende del carácter reservado del dato, de la legitimación del acceso y del perjuicio.

-COACCIONES (art. 172), AMENAZAS E INJURIAS, cometidos mediante el correo electrónico o mensajes de teléfono móvil.

Para determinar el autor es necesario no sólo identificar el IP y el titular del terminal, sino el usuario y si fue él quien lo usó para tal fin.

Si se cuestiona la autenticidad del correo o mensaje aportado por el/la perjudicada, habrá que practicar una pericial informática.

Se admite dentro del concepto de violencia (coacciones) la llamada "violencia espiritualizada", entendido como fuerza sobre la voluntad o enfrentamiento contra la libertad de actuación de otra persona, que va más allá del resultado meramente descriptivo de impedir algo a otro, caben perfectamente los casos de resistencia pasiva, de hostigamiento o de acoso, o de fuerza material en las cosas.

- QUEBRANTAMIENTO DE MEDIDA CAUTELAR o PENA.ART. 468.2

Cuando se quebranta mediante Messenger o correo electrónico la prohibición de comunicación impuesta de un cónyuge respecto a otro (ej.) la estrategia defensiva normalmente será impugnar la autenticidad de esos mensajes.

Para comprobar de donde proceden y que no han sido manipulados se debe librar un Oficio a la Policía para que averigüen la IP del terminal de donde proceden, su titular, y si es necesario un volcado del disco duro y la verificación de información en los Servidores.

Si no se han practicado ninguna de estas pruebas, tales documentos no tendrán un valor probatorio autoevidente pero sí podrán reforzar la versión del/la denunciante, si es creíble para el juzgador.

-DESCUBRIMIENTO DE SECRETOS DE EMPRESA. ART. 279 CP. DAÑOS POR VIRUS INFORMATIVOS (art. 263 y 264 CP)

*Cesión de secretos de empresa y daños por borrado de archivos informáticos.

El art. 279 CP castiga la difusión, revelación o cesión del secreto de empresa.

Lo pueden cometer además de empleados los socios o administradores.

Secreto de empresa ha sido definido por la Jurisprudencia como los relativos altivos desde el punto de como los propios de la actividad empresarial que de ser conocidos pueden afectar a su competititividad. Se incluyen no sólo los datos contables sino incluso los archivos de clientes.

En muchas ocasiones este delito va acompañado del delito de daños, al haber borrado ficheros informáticos del ordenador donde trabajaban.

Será prueba fundamental la intervención y análisis informático de los ordenadores donde estaban los archivos y en su caso, de los existentes en el domicilio o la nueva empresa creada por los empleados o socios.

***Daños por difusión de virus informáticos ("piratas o hackers").**

Se trata de programas cuya única finalidad es producir un deterioro o destrucción del "software" de aquellos terminales que infectan, o sencillamente una alteración de su sistema operativo, que determina un funcionamiento anómalo o deficiente.

La prueba de la autoría será indiciaria (titular teléfono desde el que se inicia la difusión, posesión de material informático, etc.)

Más compleja es la prueba del perjuicio a los usuarios infectados y a la compañía telefónica para restaurar el sistema.

-ESTAFA INFOMÁTICA (art. 248.2 CP).

Se incluyen los casos de "phising":los llamados hackers descubren claves y datos bancarios de personas físicas o jurídicas que operan desde internet, les extraen de sus cuentas corrientes ciertas cantidades de dinero, que las ingresan en una cuenta personal de un colaborador, que hace de intermediario o "Mula", el cual la reenvía a una cuenta corriente en un país del Este de Europa a través de Western Union, Money Gram o empresa similar, recibiendo a cambio cierta cantidad de dinero, consistente en un sueldo más un tanto por ciento de las cantidades reenviadas al extranjero.

Será necesario investigar la IP del origen de la transferencia y también la identidad del beneficiario de la misma, y lo que más frecuentemente alega éste es ausencia de dolo, al pretender disfrazarlo como un contrato laboral de intermediación en la transferencia de dinero.

-FALSEDAD DOCUMENTAL.

***En documento mercantil. Art. 392.** Se comete si se manipulan archivos informáticos para crear un documento destinado a crear una apariencia jurídica de verdadero en el ámbito mercantil.

***en documentos oficiales, como DNI, permisos de residencia, permisos de conducir, usando material informático (**discos duros externos, memorias USB, ordenador Portátil, Plastificadora e impresora).

***Falsif. Tarjetas de crédito 399 bis.** La incorporación de datos obtenidos fraudulentamente en la banda magnética de las tarjetas de crédito o débito pasó, con la reforma de la LO 5/2010, de castigarse como falsificación de moneda del art. 386 Cp a hacerlo como un delito autónomo tipificado en el art. 399 bis, si bien con pena más favorable al acusado.

-COMISIÓN DE diversos DELITOS A TRAVES DE LAS REDES SOCIALES.

*Comentarios en Tuenti.

Para que la obtención de la prueba sea lícita: No es necesaria la autorización judicial para acceder al contenido informático, pero sí es necesaria la autorización judicial para identificar al usuario de la dirección IP.

Para considerar cumplido el concepto de "difusión" se utilizan los mismos criterios que en el uso de programas de intercambio de archivos peer to peer.

DELITOS SOCIETARIOS

1.- REGULACION: ARTÍCULOS 290-297 CÓDIGO PENAL.

Art. 290 C.P. Falsedad.
Art. 291 C.P. Imposición de acuerdos abusivos.
Art. 292 C.P. Imposición o aprovechamiento de acuerdos lesivos.
Art. 293 C.P. Obstaculización de los derechos del socio.
Art. 294 C.P. Obstrucción de actuaciones inspectoras o supervisoras.
Art. 295 C.P. Administración desleal.
Art. 296 C.P. Condición de procedibilidad.
Art. 297 C.P. Definición legal de Sociedad.

Bien jurídico protegido: Seguridad del Tráfico Mercantil, así como los intereses económicos de las sociedades, de sus socios y de quienes se relacionan con ellas.

2.- CARÁCTER RESIDUAL Y SUBSIDIARIO DE LA REGULACIÓN PENAL DE ESTE TIPO DE DELITOS EN COMPARACIÓN CON LA REGULACIÓN CIVIL DE LA MATERIA.

En este punto podemos distinguir tres apartados que evidencia la dificultad de aplicar estos tipos penales, a saber: 1)- el principio de intervención mínima del derecho penal, que propugna la aplicación del mismo cuando no sea posible acudir a cualquier otra jurisdicción para la solución del conflicto; 2)- la existencia de procedimientos civiles que amparan conductas similares a las previstas penalmente; y 3)- dentro del ámbito puramente penal, la existencia de concurso entre los delitos societarios con otros delitos comunes previstos en el Código Penal lo que dificulta su aplicación.

Vamos a desarrollar cada uno de estos puntos.

A.- Principio de intervención mínima del derecho penal.

Principio de Subsidiariedad y naturaleza fragmentaria del derecho penal.

Solo cuando se constaten indicios de contenido delictivo añadido al ilícito mercantil o administrativo se aplicará la jurisdicción penal: si no, es aconsejable la remisión a otra jurisdicción.

Se hace necesario que exista una interpretación diferenciadora en cuanto al comportamiento y si no es posible, no procede acudir al derecho penal.

Algunos tipos coincide derecho penal y derecho sancionador: Art. 290 y 294 C.P.

En la legislación civil y mercantil encontramos normas que castigan los mismos comportamientos que prevén las normas penales e incluso algunos más graves, a saber:

Art. 99 Ley del Mercado de Valores:

Suministrar a la CNMV datos inexactos o no veraces, o información engañosa o que omita maliciosamente aspectos o datos relevantes;

Intervención en o realización de operaciones que impliquen simulación de trasferencias de titularidad;

Negativa o resistencia a la actuación inspectora de la CNMV;

Art. 4 ley de Disciplina e intervención de Entidades de Crédito:

Carecer de contabilidad o llevarla con irregularidades esenciales que impidan conocer la situación patrimonial y financiera;

Negativa o resistencia a la actividad inspectora;

Falta de veracidad de los datos o documentos remitidos que dificulte la apreciación de la solvencia.

Art. 40.3 de la Ley de Ordenación y Supervisión de los Seguros Privados:

Anomalías sustanciales en la contabilidad que impidan conocer la situación económica, patrimonial y financiera;

Falta de veracidad de los datos o documentos suministrados a la Dirección General de Seguros;

Excusa, negativa o resistencia a la actividad inspectora;

Incumplimiento del deber de veracidad informativa a los socios, asegurados y público.

B.- **Existencia de otros procedimientos civiles como nulidad de acuerdos sociales y responsabilidad de administradores.**

Convocatoria de la Junta: art. 100 y 101 LSA: Están obligados a convocarla los Administradores; pueden hacerlo los socios que sean titulares de al menos el 5%del capital social y en caso de negativa pueden acudir a la convocatoria judicial.

A este respecto la STS 14/07/2006 señala: "La falta de convocatoria de la Junta es una irregularidad formal que tiene su más lógica y racional solución en el ejercicio de la acción de nulidad de acuerdos sociales, sin necesidad de acudir al derecho penal".

Derecho de información: Art. 112 LSA: cualquier socio puede exigir del administrador 7 días antes de la celebración de la Junta que le informe por escrito sobre el orden del día y el contenido de la Junta. En caso de negativa, se puede acudir al Juez ordinario.

Hay que ponerlo en relación con el artículo 293 del Código Penal. En este sentido, la STS 26/11/2002 señala:"Falta un plus de antijuricidad material que justifique la respuesta penal frente al incumplimiento de obligaciones mercantiles que pueden ser demandadas igualmente en esta vía, advirtiéndose que la estructura de la obligación sería idéntica en uno y otro caso". En un intento de establecer una diferenciación se ha llegado a decir que existirá delito cuando la negativa a la información sea una actuación reiterada del administrador, pero se ha acabado concluyendo que este requisito no lo exige expresamente el tipo penal. (STS 91/13, de 1 de febrero). Igualmente, se ha querido ver la existencia del delito en: "la omisión de información tiene la intencionalidad o finalidad de impedir al socio el conocimiento de la vida de la sociedad o privar de la posibilidad de ir a la Junta".

Impugnación de acuerdos sociales: art. 115 y siguientes LSA.

Nulos: contrarios a la ley.

Anulables: se opongan a los Estatutos, lesionen intereses de la sociedad en beneficio propio o ajeno.

Caducidad: Nulos: 1 año. Anulables: 40 días.

Procedimiento: Juicio Declarativo Ordinario.

A veces, una vez transcurridos estos plazos por dejadez, la única vía posible es acudir a la jurisdicción penal.

Responsabilidad de los Administradores: art. 133 LSA. Más severa en sus conseconsecuencias que la regulación penal.

Ley Concursal: Art. 163 y siguientes: Fortuita o culpable. Expresamente regula los supuestos en que la quiebra debe calificarse como culpable.

Exige la intervención del Ministerio Fiscal.

Además, la existencia de **Tasas** en la jurisdicción civil y no en la penal, provocará que se acuda primeramente a la jurisdicción penal, que por definición es la ultima ratio.

C.- Concurso con otros delitos (apropiación indebida, falsedad, etc).

A este respecto debemos centrarnos en dos cuestiones de concurso entre distintos delitos del Código penal:

1.-Concurso entre Apropiación Indebida (art.252)- Administración desleal (Art. 295).

Se trata de una cuestión muy discutida que ha generado una jurisprudencia consolidad desde el año 1998 hasta nuestros días. Así cabe destacar las STS 4-4-13; 1-2-13; 26-2-98. Expresamente se ha recogido: "la diferenciación entre la apropiación indebida y el delito societario no ha resultado sencilla. La existencia de una aparente superposición entre la respectiva porción de injusto abarcada por ambos preceptos, ha dificultado su exégesis, existiendo resoluciones de esta Sala que se han esforzado, no siempre desde la misma perspectiva, en ofrecer una pautas interpretativas dotadas de seguridad y certeza. Conviene por ello aludir a la existencia de una línea jurisprudencial que explica que la relación entre ambos preceptos se entiende y soluciona a partir de un aparente concurso de normas que ha de ser resuelto con arreglo al criterio impuesto por el principio de alternatividad, esto es, conforme al delito que ofrece mayor pena. Debe tenerse en cuenta que el artículo 295 ha venido a

complementar las previsiones sancionadoras del artículo 252, pero no a establecer un régimen sancionador más benévolo para hechos que se consideraban y se consideran delitos de apropiación indebida, en el supuesto de que los mismos se perpetran en un contexto societario. Será inevitable en adelante que ciertos actos de administración desleal p fraudulenta sean subsumibles al mismo tiempo en el artículo 252 y en el artículo 295 del Código Penal vigente, porque los tipos en ellos descritos están en una relación semejante a la de círculos secantes, de suerte que ambos artículos se solapan. Pero este concurso de normas, se ha de resolver, de acuerdo con lo dispuesto en al artículo 8.4 del Código Penal, es decir, optando por el precepto que imponga la pena más grave. No faltan sin embargo resoluciones que han buscado un criterio de diferenciación entre la deslealtad en que incurren los autores de la acción prevista en el artículo 252 del Código Penal y la que está presente en el artículo 295, atendiendo para ello a los límites del título jurídico en virtud del cual se efectúa el acto dispositivo. Este último delito se refiere a los administradores de hecho o de derecho o a los socios de cualquier sociedad constituida o en formación que realicen una serie de conductas causantes de perjuicios, con las funciones propias de su cargo. Esta última exigencia supone que el administrador desleal del artículo 295 actúa en todo momento como tal administrador, y que lo hace dentro de los límites que procedimentalmente se señalan a sus funciones, aunque al hacerlo de modo desleal en beneficio propio o de tercero, disponiendo fraudulentamente de los bienes sociales o contrayendo obligaciones a cargo de la sociedad, venga a causar un perjuicio típico. El exceso que comete es intensivo, en el sentido de que su actuación se mantiene dentro de sus facultades, aunque indebidamente ejercidas. Por el contrario, la apropiación indebida, conducta también posible en los sujetos activos del delito de administración desleal del artículo 295, supone una disposición de los bienes cuya administración ha sido encomendada que supera las facultades del administrador, causando también un perjuicio a un tercero. Se trata por tanto de conductas diferentes, y aunque ambas sean desleales desde el punto de vista de la defraudación de la confianza, en la apropiación indebida la deslealtad supone una actuación fuera de lo que el título de recepción permite, mientras que en la otra, la deslealtad se integra por un ejercicio de las facultades del administrador que, con las condiciones del artículo 195, resulta perjudicial para la sociedad, pero no ha superado los límites propios del cargo de administrador. De acuerdo con esta idea, es perfectamente posible resolver la aplicación de los artículos 252 y 295 del Código Penal sin necesidad de acudir a la solución sugerida por la existencia de un aparente concurso de normas. Se trata de preceptos que no implican una doble valoración de un mismo hecho típico. En uno y otro caso, existiría una visible diferencia respecto del significado jurídico del desbordamiento de los poderes conferidos al administrador individual o societario".

Diferencias: Art. 295 C.P. Exceso intensivo: dentro de sus facultades.

Art. 252 C.P. Exceso Extensivo: extralimita sus facultades. (STS 11-7-05.)

2.- Concurso entre Falsedad: art.290 y 390 C.P.

Sentencia FILESA: 28-10-97: FACTURAS DE CONTENIDO FALSO.

Diferencia falsedades intelectuales o ideológicas y materiales. La falsedad material exige alguno de los tres primeros supuestos del artículo 390.1 del Código Penal, alteración del documento, mientras que la falsedad intelectual o ideológica se refiere a expresar un concepto en el documento distinto al real. Así, en el caso FILESA, aplicó el delito de falsedad documental consistente en simular un documento a unos particulares que habían emitidos facturas de contenido falso, es decir, se trataba de documentos que no responden en ningún caso a lo que su contenido manifiesta. Las facturas en cuestión fueron emitidas por representantes de unas sociedades existentes contra otras, en algunos casos muy notorias, y pagadas efectivamente por éstas, aunque no por causa de los servicios, trabajos o prestaciones que en ellas figuraban, sino para financiar ilegalmente al partido político entonces gobernante.

Posteriormente la STS 26-2-98 (Agencia Trust):consideró que la falsedad ideológica no debe reputarse como delito de falsedad documental.

Ante esta controversia y contradicción conviene recordar el Acuerdo del Pleno Sala 2º T.S. 26-2-99: que concluye que se debe castigar como delito de falsedad documental también la falsedad intelectual y no solo la material.

Igualmente la Consulta F.G.E 15/97, 16 diciembre estableció los siguientes criterios:

1.- falsedad cometida por particulares no incluye falsedad intelectual art. 390.4.
2.- Verbo falsearen del art. 290 comprende todas las conductas del art. 390, también el nº 4.

3.- Concurso de leyes: artículo 8.1 principio de especialidad, se aplicaría el art. 290 C.P.

4.- Si no es aplicable el art. 290 porque falte algún requisito, se aplica la falsedad del art. 392 pero solo en alguna de las tres modalidades del art. 390, no en la 4º.

3.- CONCEPTO DE SOCIEDAD EN ESTE TIPO DE DELITOS.

Art. 122 C.CO.

Enumeración establecida legalmente: Muchas críticas.

No aclara nada. Si se establece un concepto es para que permita diferenciarlo de los ya existentes en el ámbito civil y mercantil.

Reiterativa: Cooperativa es sociedad mercantil.

Caja de Ahorros es entidad financiera o de crédito.

Númerus Apertus: pero teniendo en cuenta que nos encontramos ante la jurisdicción penal la interpretación debe ser restrictiva.

Finalidad común: Para el cumplimiento de sus fines participe de modo permanente en el mercado.

Peculiaridades en cuanto a determinados entes sociales:

Sociedades en formación: artículo 15 LSA.

Sociedad Irregular: art. 16 LSA.

Fundaciones: finalidad no lucrativa por definición.

Sociedad en liquidación: STS 21/02/13 Juzgado de Algeciras. En un supuesto en que tras la disolución y en fase de liquidación la administradora vendió los bienes y productos de la empresa destinada a mobiliario y decoración a su marido que también tenía una empresa con el mismo objeto social, el Tribunal señalo expresamente que se comete el delito societario de administración desleal aun cuando la sociedad esté en liquidación, ya que en esta fase, los bienes sociales están destinados a sufragar las deudas y pagar a los acreedores.

Entidades de Crédito: PROBLEMA DE LAS PREFERENTES.

Sociedades civiles y comunidad de bienes: excluidas.

En cualquier caso, existe mucha controversia y el Código Penal, lejos de aclarar los términos, ha venido a introducir mucha más confusión al respecto.

4.- **AUTORÍA: ADMINISTRADOR DE HECHO Y DE DERECHO**.

Artículo 31 C.P. (anterior Art. 15bis).

No supuesto de responsabilidad objetiva. En este sentido la STC 253/93, de 20 de julio, con cita de la STC 150/89 señala: "Su incorporación al Código no vino en modo alguno a introducir una regla de responsabilidad objetiva que hubiera de actuar indiscriminada y automáticamente, siempre que, probada la existencia de una conducta delictiva cometida al amparo de una persona jurídica, no resulte posible averiguar quiénes, de entre sus miembros, han sido los auténticos responsables de la misma, pues ello sería contrario al derecho a la presunción de inocencia y al propio tenor del precepto. Lo que el mismo persigue, por el contrario, es obviar la impunidad en que quedarían las actuaciones delictivas perpetradas bajo el manto de una persona jurídica por miembros de la misma perfectamente individualizados, cuando, por tratarse de un delito especial propio, es decir, de un delito cuya autoría exige necesariamente la presencia de ciertas características, éstas únicamente concurrieren en la persona jurídica y no en sus miembros integrantes. La introducción del artículo 15 bis del Código Penal tuvo el sentido de conceder cobertura legal a la extensión de responsabilidad penal en tales casos, y solo en ellos, a los órganos directivos y representantes legales o voluntarios de la persona jurídica, pese a no concurrir en ellos, y sí en la entidad en cuyo nombre obraren, las especiales características de autor requeridas por la concreta figura delictiva. Mas, una vez superado así el escollo inicialmente existente par poderles considerar autores de la conducta típica, del citado precepto no cabe inferir que no hayan de quedar probadas, en cada caso concreto, tanto la real participación en los hechos de referencia como la culpabilidad en relación con los mismos".

Delitos especiales: Propios: no correspondencia con uno general.
Impropios: correspondencia con uno general.

Administrador de hecho: dos supuestos: en la práctica el que maneja la sociedad.
No cumplimiento de alguno de los requisitos legales en su nombramiento o que éste haya caducado.

Se puede definir el administrador de hecho como la persona que tiene el dominio de las actuaciones de la persona jurídica.

5.- **OTRAS FORMAS DE PARTICIPACIÓN**.

A pesar de encontrarnos que los delitos societarios son delitos especiales, el Tribunal Supremo ha señalado reiteradamente que deben contemplarse en estos delitos otras formas de participación. Y así, ha señalado: "En cuanto al sujeto activo de estos tipos penales, es criterio jurisprudencial pacífico y reiterado, por analogía con el alzamiento de bienes, que no sólo los que ostentan la condición de deudores (en el

presente caso, administradores), pueden ser autores del delito, sino también quienes colaboren con ellos en auxilio necesario cuando haya habido confabulación" (STS 17/10/1981, 16/12/1982 y 27/12/2007).

Debido a la peculiaridad del fenómeno societario debemos diferenciar dos grandes supuestos en los que la operativa es radicalmente distinta, por un lado, las grandes sociedades formadas por grupos de empresas, y por otro lado, las pequeñas sociedades y sociedades familiares.

A.- **Grandes sociedades**: Son fruto del fenómeno de la Globalización, con actuación a nivel internacional.

Diferenciar: los que deciden y los que ejecutan.

Superar el concepto puramente objetivo-formal de autor: no necesariamente realizar actos de ejecución. Extender el concepto de autor.

En este tipo de sociedades son más importantes los centros de decisión que los centros de ejecución.

Estaríamos ante un supuesto de Autoría mediata, cuando el que ejecuta no decide ni conoce el alcance o relevancia penal de lo que hace. (No inductores).

Coautoría: dos supuestos: 1.- si el ejecutor conoce y decide lo acordado por otros.

2.-Consejo de administración: Todos los miembros que han votado el acuerdo, no obstante, habría que excluir de responsabilidad si algún miembro vota en contra.

CONSEJOS DE ADMINISTRACIÓN: posibilidad de comisión por omisión, deber de vigilancia y de lealtad como administradores.

Cooperadores necesarios y cómplices: Asesores, contables, peritos, etc. (personas con conocimientos especiales). CASO MESSI.

Delitos fiscales: la falsedad absorbida por el delito fiscal.

EEUU: Fiscales ofrecen impunidad a los asesores, contables, etc, para que colaboren y delaten a los peces gordos.

B.- **Pequeñas empresas o empresas familiares**.

Administrador de hecho y de derecho. (¿aparece como excluyente o responsabilidad de ambos?)

Problema: administrador legal el cónyuge que no sabe nada: responsabilidad penal o no. CASO INFANTA.

Cumplimiento de normas mercantiles: hay situaciones en las que durante mucho tiempo se ha consentido por todos los socios la falta absoluta de cumplimiento de la normativa propia de la sociedad a la que pertenecen, lo que les deslegitima para reclamar después penalmente dicho incumplimiento.

Papeles los lleva una gestoría: quien incumple el derecho de información.

6.- **REQUISITO DE PROCEDIBILIDAD EN ESTE TIPO DE DELITOS.**

Necesidad de denuncia. No exige querella.

Distinto de las personas legitimadas para impugnar acuerdos sociales.

Interés General.