Revista Penal México 11-12
Doctrina
Núms. 11-12, septiembre de 2016-agosto de 2017

Ciberterrorismo: la nueva cara de la delincuencia en el siglo XXI. La participación y fomento al delito por órganos de gobierno y empresas

Alberto Enrique Nava Garcés

Profesor investigador del Inacipe. Miembro del núcleo académico básico del Infotec

Resumen: *Dada la capacidad que tiene el ciberterrorismo para desestabilizar economías y Estados completos al producir ataques en sistemas informáticos que controlan los más diversos ámbitos, se hace necesario revisar los términos legales que lo delimitan, y más específicamente, los tipos penales que buscan sancionar estas conductas. En México, es indispensable revisar la legislación, ya que ésta indica que para configurar el tipo de terrorismo se requiere la comisión de los hechos por medios violentos; considerando que el ciberterrorismo se apoya en medios electrónicos para cumplir sus objetivos, resulta difícil atribuir responsabilidad, particularmente cuando la autoría podría residir en personas morales, en países ajenos o cuando es inclusive alentada o cometida por los mismos órganos o grupos de poder del Estado.*

Palabras clave: *Ciberterrorismo, ataques informáticos, medios comisivos, estigmatización.*

Abstract: *Considering cyber terrorism is able to disrupt economies and entire States by producing attacks against relevant information systems, becomes necessary to make a review of the legal terms and, more specifically, of the basic criminal definition in order to sanction this conducts. In Mexico is essential to reform the law, because it establishes as a terrorism requirement that certain conduct has been committed with violence; if cyber terrorism is supported in the use of electronic media it becomes difficult to probe their responsibility, particularly when perpetrators comes from legal entities, from other countries o when the terrorist act has been instigated or committed by powerful people close to government.*

Key words: *Cyber terrorism, attacks against information systems, means of commission of the crime, stigmatization.*

Rec: 10-05-2017 | **Fav:** 30-06-2017 | **Código ORCID:** orcid.org/0000-0002-1025-0850

1. Ciberseguridad, economía y ciberterrorismo

El ciberterrorismo es un concepto utilizado de modo frecuente para referirse a una diversidad de ataques en contra de las comunicaciones, la información y de los sistemas informáticos que la contienen. El tamaño del problema es proporcional al tipo de sistema que puede ser afectado y la dependencia que exista para la continuación de los trabajos diarios.

Las comunicaciones estratégicas, los sistemas de salud, el control aéreo, la videovigilancia, los transportes con sistema computarizado, las armas controladas por sistemas de cómputo, la georreferenciación de vehículos, los objetos que requieren de conexión a la red, las propias redes sociales, los bancos de datos, los sistemas financieros, la telefonía, los mensajes de texto, internet, etc., son solo algunos ejemplos de los objetivos que el ciberterrorismo persigue para su anulación temporal o definitiva.[1]

Es por tal motivo que, cuando nos referimos a esta figura en particular, confluyen distintas materias para su estudio: la economía, el Derecho penal, la ciberseguridad, entre las principales (fig. 1).

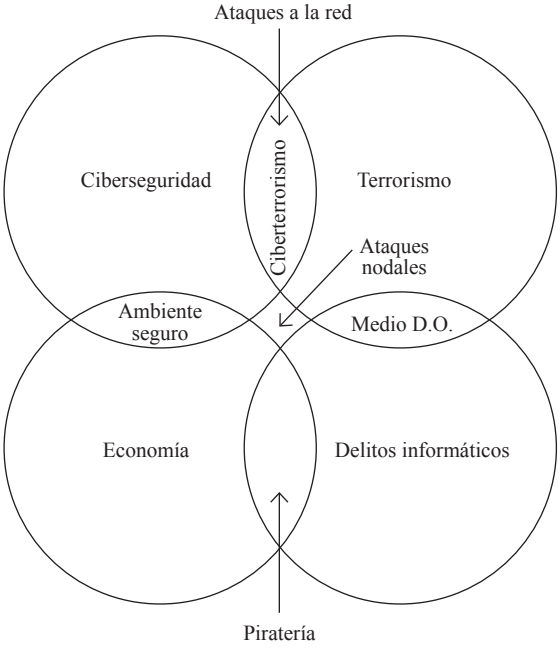

Figura 1

[1] **"La Guerra del siglo XXI ya está aquí; daños que provocan las armas cibernéticas** *(BBC Mundo)*.- No sabían qué estaba pasando. El equipo se dañaba constantemente, pero la causa era un misterio. Lo reemplazaban, pero volvía a ocurrir.

Transcurrió un año antes de que se descubriera que el problema era que un gusano informático llamado Stuxnet había infectado los sistemas electrónicos de la planta de enriquecimiento de uranio de Natanz, en Irán. Esa era la razón de las fallas que le causaron daños y retrasos al programa nuclear iraní.

El descubrimiento de Stuxnet, en 2010, evidenció que los crímenes cibernéticos podían ir más allá del espionaje y el robo de datos personales con un fin económico: confirmó que se podían ocasionar daños físicos con una motivación política.

"Fue la explotación exitosa del ciberespacio con el objetivo de controlar una serie de procesos industriales para destruirlos de manera remota, sin que mediara ningún tipo de confrontación militar", indica Lior Tabansky, especialista en ciberseguridad estratégica de la Universidad Yuval Ne'eman, en Israel, en la publicación *Cyber Security Review*.

Y añade: "Demostró cuan sofisticadas y precisas pueden ser las armas cibernéticas". El incidente en Ivano-Frankivsk, en Ucrania, dejó sin electricidad a 230,000 personas.

Es difícil saber con certeza cuál fue el origen de ese ataque, pero según un artículo del Instituto de Tecnología de Massachusetts (MIT, por sus siglas en inglés), en Estados Unidos, se sospecha que un equipo de expertos israelíes y estadounidenses estuvo involucrado en el incidente.

Esta opinión es compartida por diversos especialistas en seguridad informática.

Este tipo de incidentes, que afectan el funcionamiento de equipos e infraestructuras, es una de las modalidades de ciberataques más peligrosa. En años recientes se han registrado varios de distinta naturaleza. Pero sus consecuencias van más allá del plano físico.

"Aparte del daño concreto, este tipo de eventos tienen un efecto secundario muy importante: el psicológico. A eso se refieren los términos ciberterrorismo y ciberguerra", le dice a BBC Mundo Graham Fairclough, especialista del Centro de Ciberseguridad de la Universidad de Oxford, en el Reino Unido.

Y explica: "Generan miedo y ansiedad. Se tiene la sensación de que alguien puede hacerte algo y que no tienes la posibilidad de protegerte. El tema del alcance también es importante, en el ciberespacio la distancia física no es relevante. Puedes ser una víctima aunque estés lejos del punto de origen del ataque".

En este contexto, el individuo pierde confianza en el sistema y en su habilidad para protegerlo.

"Todo lo que funcione con un programa informático puede utilizarse para causar daño, bien sea algo tan sencillo como una nevera o algo mucho más complejo. La clave es el código, que se puede desarrollar o comprar a criminales en internet, los equipos físicos (hardware) se pueden adquirir con facilidad en la red", señala Fairclough. […]

Ataque impresionante

Un caso que grafica la sofisticada fusión entre lo físico y lo psicológico es el sorprendente ciberataque que sufrió el sistema eléctrico de Ivano-Frankivsk , una ciudad en el oeste de Ucrania en diciembre de 2015.

Sin ningún tipo de advertencia, los técnicos del centro de control que abastece de electricidad a la zona, perdieron el control de sus computadoras. El cursor del ratón empezó a moverse solo en la pantalla y a desactivar los interruptores que controlan el suministro.

En el primer círculo encontramos lo relativo a la ciberseguridad consistente en el cuidado que tiene un Estado para resguardar la información y las comunicaciones. Por eso, cuando este círculo cruza con la economía, podemos considerar que estamos ante el escenario ideal donde la misma se resguarda. Por el otro lado tenemos los delitos comunes, que cuando cruzan con la economía, afectan esferas económicas o industriales como la intelectual (piratería). Arriba a la derecha, el terrorismo, como figura del Derecho penal, pone en riesgo la ciberseguridad y es exponencialmente más dañina que la delincuencia común, por lo que el cruce de estos círculos lleva a las actividades de la delincuencia organizada y paulatinamente a los sitios que ocupa la *deep web*.

Cuando estos círculos chocan, dan lugar al ciberterrorismo y a los ataques nodales (contra actividades estratégicas para un país).

1.1. Concepto

Acuñar el término ciberterrorismo como la posibilidad de que sean atacados tanto los sistemas de información como las redes de datos o que estos sean utilizados por y para perpetrar actos terroristas, resulta poco afortunado, ya que todos los términos que utilizan el prefijo "ciber" no son del todo exactos en tanto el objeto que pretenden describir.

La cibernética nos remite a una de las áreas más avanzadas en donde interviene la computación,[2] sin embargo se trata de un proceso de retroalimentación, ya sea mecánico, biológico o electrónico.

A través de la cibernética se busca el control de un proceso, de ahí que su etimología haga referencia a un timonel. La cibernética enlaza a la teoría general de sistemas con el Derecho, cuando éste es visto como un sistema del que se desprenden (y a la vez lo componen) diversos subsistemas autopoiéticos.

"Dos años antes de que Bertalanffy lanzara su teoría, el matemático Wiener inició sus estudios sobre el control y la comunicación: bautizó su trabajo basándose en el vocablo griego *kybernetes* (arte del timonel). Su obra, *Cybernetics, or control and communication in the animal and machine*, fue publicada en 1948 y expone los temas fundamentales de la nueva disciplina".[3]

De esta raíz parte la acuñación del vocablo *iuscibernética*, el cual fue propuesto en 1968 por el profesor italiano Losano. Con este nuevo nombre, Losano pretendía reorganizar todo lo relacionado con la Cibernética y el Derecho, pues la fusión interdisciplinaria, característica de la Cibernética, en el sector jurídico había terminado por transformarse en confusión de disciplinas.

El término *ciberespacio* fue acuñado por el escritor William Gibson (en 1984) y "es una metáfora para describir el terreno no físico creado por sistemas de computadora".[4]

Lawrence Lessig, en su libro *Code and other laws of cyberspace*, nos indica que

> El ciberespacio no es un lugar. Es muchos lugares distintos. La forma de estos muchos lugares no es idéntica. Está conformado de diferentes maneras, esto resulta fundamental. Estas diferencias resultan en parte por la gente que puebla los diversos lugares que lo conforman, pero la situación demográfica no puede por sí sola explicar estas variantes. Hay en el ciberespacio la conjunción de más elementos y variables que día a día lo van creando, modificando. Algo lo hace variable.[5]

Aun cuando se ha adoptado la referencia al ciberespacio como un sinónimo de lo que acontece en la

Los hackers que estaban detrás del ataque sacaron a los técnicos del sistema e impidieron que volvieran a conectarse cambiando sus contraseñas.

¿El resultado? Según un reportaje de la publicación especializada en tecnología *Wired*, 230,000 residentes se quedaron sin luz y sin calefacción durante varias horas. 30 subestaciones fueron apagadas, al igual que dos centros de distribución energética, lo que prácticamente duplicó el número de subestaciones fuera de servicio.

Un evento similar fue reportado en diciembre de 2016, en esta oportunidad en el norte de la capital ucraniana, Kiev.

Funcionarios gubernamentales responsabilizaron a Rusia por ambos eventos, que ocurrieron en el marco del enfrentamiento que existe entre ambos países desde hace aproximadamente tres años, tras la anexión a Rusia de Crimea, una península que se encuentra al sur de Ucrania. http://www.insightmx.com.mx/detallenota.php?id_news=125 consultado el 16 de abril de 2017; 17:30 h

[2] Cfr. Vasconcelos Santillán, Jorge, *Informática I, Computación Básica*, 1ª. ed., Publicaciones Cultural, México, 2002, p. 106.

[3] Guibourg, Ricardo A., *Informática Jurídica Decisoria*, Astrea, Buenos Aires, 1993, p. 16.

[4] Consultable en: http://www.webopedia.com/TERM/c/cyberspace.html

[5] Lessig, Lawrence, *Code and other laws of cyberspace,* Basic books, U.S.A. 1999, p. 63, "Cyberspace is not a place. It is many places. The character of these many places is not identical. They instead differ in ways that are fundamental. These differences come in part from differences in people who populate these places. But demographics alone won't explain the variance. Something is going on".

red y de ahí surgen sus derivaciones tales como ciberterrorismo, sigo insistiendo en el término delito informático (relativo a la información) o a su género "delito electrónico" dentro del cual se podría inscribir el terrorismo con esta nueva modalidad. Jesús Edmundo Coronado Contreras define:

> Ciberdelito o crimen cibernético puede ser definido como aquel delito en el que redes computacionales pueden ser un objetivo o una herramienta substancial.[6] Una gran variedad de definiciones existen en la bibliografía sobre el tema, la mayoría de ellas se basan en el contenido de la Convención contra la Ciberdelincuencia adoptada por el Consejo de Europa; ciberdelito es el acto criminal cometido utilizando redes de comunicación electrónicas o sistemas de información o actos en contra de esas redes y sistemas.
>
> Existen varias clasificaciones sobre lo que se puede considerar un "ciberdelito". Una de ellas es la que identifica la actividad delictiva:
>
> 1. Delitos en un dispositivo (pornografía infantil)
> 2. Delitos usando un dispositivo (fraude)
> 3. Delitos contra un dispositivo (acceso ilegal o no autorizado).[7]
>
> A nivel internacional existen algunos informes y reportes tanto del G-8 como de la Organización de las Naciones Unidas (ONU). En 1999, la ONU realizó un extenso reporte titulado "*International Review of Criminal Policy*". En 2005 fue realizado en la ciudad de Bangkok, Tailandia, un taller en el tema dentro del Onceavo Congreso de las Naciones Unidas en Prevención del Delito y Justicia Criminal. Recientemente en 2013, la Oficina de las Naciones contra la Droga y el Delito (UNODC por sus siglas en inglés) efectuó un estudio en el tema titulado "*Comprehensive Study on Cybercrime*".
>
> […]

Barry Colin, miembro del *Institute for Security and Intelligence* en California, es a quien se le atribuye la creación del término "ciberterrorismo", definiéndolo como la fusión entre cibernética y terrorismo. Maura Conway lo define como la convergencia entre ciber delito y terrorismo.[8] Ataques y amenazas contra dispositivos, sistemas e información resguardada con el propósito de intimidar a un gobierno o a su población en cumplimiento de objetivos políticos o sociales. Considerar un ataque como "terrorista" requiere que sea resultado de violencia contra una persona o propiedad con la intención de cuasar un daño severo o por lo menos inspirar terror.

Otros autores son más específicos al referirse a que "ciberterrorismo" puede ser cualquier ataque electrónico desde el ciberespacio desde redes internas y externas, en particular Internet, inspirado en diferentes motivos y dirigido a objetivos en particular.[9]

Terrorismo cibernético puede referirse a ataques premeditados y de inspiración política realizados por grupos o agentes clandestinos en contra de información, sistemas computacionales, programas y demás datos informáticos que resulten en actos de violencia hacia objetivos no beligerantes.[10] En ese sentido habría de distinguir cuando los considerados "terroristas" utilizan computadoras o sistemas informáticos para sus actividades (ejemplo de ello es el uso terrorista de Internet) y cuando dichos instrumentos son un objetivo en concreto.[11]

La preocupación de quienes han abordado este tema, los ha llevado a cometer el yerro de identificar al terrorismo por internet con una comunidad religiosa y, de manera equívoca, estigmatizan a los miembros de un culto adosándoles el término de terroristas por los supuestos idearios con los que se hacen propaganda algunos grupos terroristas. El Islam ha sido el pretexto de los grupos terroristas, pero

---

[6] Koops, Bert-Jaap. "The Internet and its Opportunities for Cybercrime", 2010, p. 737

[7] Hargreaves C. y D. Prince. "*Understanding Cyber Criminals and Measuring Their Future Activity Developing cybercrime research"*, Security Lancaster, Lancaster University. Disponible en: http://eprints.lancs.ac.uk/65477/1/Final_version_Understanding_cyber_criminals_and_measuring_their_activity.pdf

[8] Conway, Maura. "*Cyberterrorism: The Story So Far"*. Department of Political Science 1, Trinity College, Dublin, Ireland, 2013. Disponible en: http://doras.dcu.ie/496/1/info_warfare_2_2_2003.pdf

[9] Jalil S.A. *"Countering Cyber Terrorism Effectively: Are We Ready To Rumble?*" GIAC Security Essentials Certification (GSEC) Practical Assignment, Version 1.4b, Option 1, junio 2003. Disponible en: http://www.giac.org/paper/gsec/3108/countering-cyber-terrorism-effectively-ready-rumble/105154

[10] Pollitt, Mark citado por Krasavin, S. *What is Cyber-terrorism?* Computer Crime Research Centre. Disponible en: http://www.crime-research.org/library/Cyber-terrorism.htm

[11] http://www.ured.org.mx/ured/breves-consideraciones-sobre-la-ciberdelincuencia-y-el-ciberterrorismo/ Consultado el 5 de mayo de 2017.

considero que ello solo ha servido para estigmatizar un credo y a quienes pertenecen al mismo.[12] Dar un sesgo religioso a las actividades ilícitas sólo genera mayor intolerancia en este mundo al que parece que no le son pocas las causas para polarizarse. Así, Cano Paños describe "El binomio internet/terrorismo islamista":

> Relacionar el terrorismo islamista con internet y analizar dicho binomio, no supone desde luego una tarea descabellada en la época actual. En una era marcada por la globalización de las comunicaciones y el uso de la red de internet por miles de millones de usuarios en todo el planeta, hace que el uso de este medio de comunicación pueda producirse con objetivos radicalmente dispares. En el concreto caso del terrorismo islamista, el uso que viene haciéndose de internet por esta denominada "ideología del odio" representada por *Al Qaeda* puede sintetizarse en los siguientes aspectos:
>
> 1.- Como instrumento para llevar a cabo o amenazar con la ejecución de ataques contra las redes computarizadas que proveen servicios públicos, tales como los sistemas de control de energía, redes de ferrocarril, aeropuertos, sistemas financieros, de seguridad, etc., es lo que se conoce como "ciberterrorismo".[13]

Como lo señalo líneas arriba, el autor en comento parece desconocer que *Al Qaeda* e *ISIS* no persiguen *per se* un objetivo religioso (aunque ésta sea su aparente bandera) sino proteger otros intereses de la región como la ruta del opio, en el primer caso y los grandes caudales generados por la guerra y el petróleo, en el segundo.

Pero más allá de estas precisiones y diferencias conceptuales, lo cierto es que la legislación sobre el tema no ha alcanzado el nivel de discusión que se merece. El tipo penal de terrorismo en el Código Penal federal se ha quedado corto al contemplar solamente los medios comisivos violentos.

1.2. Terrorismo según el Código Penal federal (México)

En las distintas latitudes de América Latina se han emitido cuerpos legales para combatir el fenómeno de la delincuencia en la red. Así también, se han creado cuerpos especializados para la investigación y loca-

---

[12] **Facebook y Google, demandados por "ayudar" al terrorismo.**
Familiares de las víctimas del ataque terrorista de San Bernardino demandaron a Facebook, Google y Twitter, por proporcionar plataformas para ayudar al grupo Estado Islámico a extender su propaganda
La demanda indica que las firmas no hacen lo suficiente para bloquear las cuentas del Estado Islámico y que, sin embargo, son beneficiadas económicamente por éstas.
Familiares de las víctimas del ataque terrorista ocurrido en San Bernardino demandaron a Facebook, Google y Twitter, empresas a las que acusaron de proporcionar plataformas para ayudar al grupo Estado Islámico a extender su propaganda, reclutar seguidores y recaudar dinero.
La demanda presentada en la corte federal de Los Ángeles argumenta que las compañías ayudaron y fueron cómplices de terrorismo, proporcionaron material de apoyo a grupos terroristas y son responsables de la muerte culposa de tres de las 14 víctimas asesinadas en el ataque del 2 de diciembre de 2015 durante un evento de capacitación y fiesta del Departamento de Salud.
Syed Rizwan Farook y Tashfeen Malik, la pareja casada que realizó el ataque con fusiles de alto poder, fueron inspirados por el grupo Estado Islámico, señalaron las autoridades. Malik había prometido lealtad al grupo a través de su cuenta de Facebook alrededor del tiempo de la masacre, en la que además resultaron heridas 22 personas.
La demanda es similar a otras contra proveedores de redes sociales que han sido presentadas en tribunales del país por muertes en ataques en la nación y en el extranjero. Los mismos abogados demandaron a las mismas empresas por la masacre ocurrida en 2016 en el club nocturno Pulse en Orlando, Florida
Algunas de esas querellas han sido desechadas porque la ley federal protege de responsabilidad a los proveedores de servicios de internet por contendido presentado por usuarios.
Facebook dijo que se compadece por las víctimas y sus familias y que retira rápidamente contenido de grupos terroristas cuando es reportado.
"No existe lugar en Facebook para grupos que se involucran en actividad terrorista o para contenido que exprese apoyo a tal actividad", señaló la compañía a través de un comunicado.
Google y Twitter no respondieron de inmediato una solicitud de comentario de *The Associated Press*.
La demanda dice que las compañías no hacen lo suficiente para bloquear o retirar cuentas del grupo Estado Islámico y que se benefician económicamente de anuncios colocados junto a mensajes del grupo extremista islámico.
"Sin los acusados Twitter, Facebook y Google (YouTube), el explosivo crecimiento de ISIS en los últimos años para convertirse en el grupo terrorista más temido del mundo no hubiera sido posible", agrega la demanda refiriéndose al grupo Estado Islámico por sus siglas en inglés. Consultado en http://www.eluniversal.com.mx/articulo/techbit/2017/05/5/facebook-y-google-demandados-por-ayudar-al-terrorismo el 6 de mayo de 2017, 17:28 hs.

[13] Cano Paños, Miguel Ángel "El binomio internet/terrorismo islamista", en *Iter Criminis,* año 4, número 21, Inacipe, Mayo-junio 2011, p. 116.

lización de los autores de tales delitos de las nuevas tecnologías, pero el caos en la legislación y las soluciones legislativas sin reflexión sólo han permitido crear un espacio de impunidad en el medio. Salvo algunas conductas focalizadas, como la pornografía infantil, las demás pueden hallar grandes vacíos legislativos y orgánicos.

En primer lugar, de acuerdo con Luciano Salellas,[14] desde abril de 2000, Argentina es sede para América del Sur de la Asociación Internacional de Comunicaciones Electrónicas de las Fuerzas Armadas (AFCEA Internacional). Se trata de una organización civil sin fines de lucro que reúne a especialistas en estos problemas (sistema C41SR, comando, control, comunicaciones, computación, inteligencia, vigilancia y reconocimiento electrónico) en el ámbito gubernamental, industrial y empresarial, de las fuerzas armadas y de seguridad, para fomentar el entendimiento, promover la eficiencia, la cooperación y el desarrollo profesional de sus miembros, a fin de lograr una verdadera evolución en el centro del campo de la información.

Por su parte, la Brigada de Investigaciones del Cibercrimen de la Policía Investigadora de Chile, consciente de los avances tecnológicos en el ámbito delincuencial, creó en octubre de 2000 la Brigada de Investigaciones del Cibercrimen, unidad especializada en la comisión de delitos vía Internet como amenazas, estafas, falsificación, pornografía infantil y delitos informáticos propiamente, entre otros.[15]

Asimismo, la Policía Nacional del Perú, División de Investigación de Delitos de Alta Tecnología, es el órgano de ejecución de la Dirección de Investigación Criminal que tiene como misión investigar, denunciar y combatir el crimen organizado trasnacional (globalizado) y otros hechos trascendentes a nivel nacional en el campo de los delitos contra la libertad, el patrimonio, la seguridad y tranquilidad públicas, la defensa y seguridad nacionales, la propiedad industrial y otros cometidos mediante el uso de la tecnología de la información y comunicación, aprehendiendo los indicios, evidencias y pruebas, así como identificando, ubicando y deteniendo a los autores con la finalidad de ponerlos a disposición de la autoridad competente.[16] El tipo penal en el Código Penal federal señala:

Terrorismo

Artículo 139.- Se impondrá pena de prisión de quince a cuarenta años y cuatrocientos a mil doscientos días multa, sin perjuicio de las penas que correspondan por otros delitos que resulten:

I. A quien utilizando sustancias tóxicas, armas químicas, biológicas o similares, material radioactivo, material nuclear, combustible nuclear, mineral radiactivo, fuente de radiación o instrumentos que emitan radiaciones, explosivos, o armas de fuego, o por incendio, inundación o **por cualquier otro medio violento**, intencionalmente realice actos en contra de bienes o servicios, ya sea públicos o privados, o bien, en contra de la integridad física, emocional, o la vida de personas, que produzcan alarma, temor o terror en la población o en un grupo o sector de ella, para atentar contra la seguridad nacional o presionar a la autoridad o a un particular, u obligar a éste para que tome una determinación.

II. Al que acuerde o prepare un acto terrorista que se pretenda cometer, se esté cometiendo o se haya cometido en territorio nacional.

Las sanciones a que se refiere el primer párrafo de este artículo se aumentarán en una mitad, cuando además:

I. El delito sea cometido en contra de un bien inmueble de acceso público;

II. Se genere un daño o perjuicio a la economía nacional, o

III. En la comisión del delito se detenga en calidad de rehén a una persona.

1.2.1. Los medios comisivos en el delito de terrorismo

Dentro de los elementos del tipo nos encontramos con un ámbito al que, por su carácter accesorio, no se le ha dado la importancia que hoy día revisten los medios comisivos, sobre todo en discusiones como la que ahora nos ocupa. En el libro *Programa de Derecho Penal*, Celestino Porte Petit, señala:

> En numerosos casos, los tipos exigen determinados medios, originándose los llamados *delitos con medios legalmente determinados o limitados*. Ello quiere decir que para que pueda darse la tipicidad deben concurrir los medios que exija el tipo correspondiente. De este modo, Mezger expresa que "por delitos con medios legalmente

[14] Luciano Salellas, "Delitos Informáticos, Ciberterrorismo, V.1.201", *Boletín Informativo de Seguridad* (http://www.cabinas.net/monografias/informatica/delitos_informativos_ciberterrorismo.pdf).

[15] Véase http://www.policia.cl/paginas/brigadas/bg-bricib/bg-bricib.htm

[16] Véase http://www.policiaiformatica.gob.pe/nosotros.asp

determinados debe entenderse aquellos tipos de delitos en los que la tipicidad de la acción se produce, no mediante cualquier realización del resultado último, sino sólo cuando éste se ha conseguido en la forma en que la ley expresamente determina [...]".
En consecuencia, el medio exigido por el tipo puede dar lugar a resultados diversos.[17]

Pero al tipo penal en cuestión le hace falta una adecuación a los tiempos que vivimos, ya que el medio que utiliza, como lo es la red, no es violento por naturaleza pero puede causar daños considerables con resultados materiales que ya podemos anticipar.

Caso 11-M

El jueves 11 de marzo de 2004, España vivió una de las jornadas más difíciles de los últimos años. Diversos trenes fueron objeto de atentados terroristas. El resumen de los hechos lo encontramos en el auto de procesamiento dictado por la Audiencia Nacional el 10 de abril de 2006. Esto es, en sólo dos años, los encargados de la investigación del delito habían logrado llevar ante los tribunales a los probables responsables. Mucho de ese trabajo fue logrado a través de las distintas evidencias electrónicas que quedaron. Las tecnologías utilizadas fueron el medio para que se actualizara el delito de terrorismo y los conexos por los que se instruyó la causa correspondiente.

Los hechos, señala el auto de procesamiento se desarrollaron de la siguiente manera:

El día **11 de marzo de 2004,** jueves, se produjeron una serie (sic) encadenada de explosiones que tuvieron lugar entre las 7 horas 36 minutos y las 7 horas 40 minutos aproximadamente en diferentes puntos de la línea de ferrocarril Cercanías de Madrid, que discurre por al área topológica conocida como "El corredor de Henares" (línea férrea que une las Estaciones del RENFE de Alcalá de Henares y de Atocha-Madrid), ocasionando 191 muertos y 1.755 heridos (en número todavía provisional), amén de innumerables daños materiales tanto en los servicios ferroviarios como en otras propiedades.

Las relaciones de personas fallecidas y heridas se reflejarán a continuación:

Los trenes afectados, todos ellos de la red de Cercanías de RENFE, fueron los siguientes, atendiendo a la hora de salida de la Estación de RENFE de Alcalá de Henares:

- **Tren n° 21431**, compuesto de seis vagones, salida de Alcalá de Henares a las 7 horas 1 minuto.
- **Tren n° 17305**, compuesto de seis vagones, salida de Alcalá de Henares a las 7 horas 4 minutos.
- **Tren n° 21435**, compuesto de seis vagones, salida de Alcalá de Henares a las 7 horas 10 minutos -este tren tenía doble altura en sus vagones-.
- **Tren n° 21713** compuesto de seis vagones, salida de Alcalá de Henares a las siete horas 14 minutos.

En este escrito remitido por **RENFE** el 27 de julio de 2005 (registrado en este Juzgado el 27/07/05), se adjuntaba documentación relativa a la situación de trenes el día 11 de marzo de 2004 en las estaciones que sufrieron los atentados.

Según la afectación de la catenaria al momento de las explosiones, la situación de los trenes el día 11 de marzo de 2004, sería la siguiente:

MADRID ATOCHA (7:36)	**(ORIGEN>DESTINO)**
21431 ESTACIONADO EN VÍA 2	(ALCALÁ H.-ALCOBENDAS)
MADRID ATOCHA (7:39)	**(ORIGEN>DESTINO)**
17305 DETENIDO ANTE SEÑAL EG	(ALCALÁ H.- CHAMARTÍN)
EL POZO (7:38)	**(ORIGEN>DESTINO)**
21435 ESTACIONADO EN EL POZO	(GUADALAJARA-ALCOBENDAS)
SANTA EUGENIA (7:38)	**(ORIGEN>DESTINO)**
21713 ESTACIONADO EN SANTA EUGENIA	ALCALÁ H.-CHAMARTÍN-MADRID P. PIO)

[17] Porte Petit Candaudap, Celestino, *Programa de Derecho Penal, Parte General,* 3ª ed., Trillas, México, 1990, p. 425.

La secuencia de explosiones en los trenes fue la siguiente, siempre atendiendo a que se numeran los vagones o vehículos en el sentido siguiente (la cabecera de tren es el 1, y la cola de tren el 6; y todos ellos sentido Alcalá de Henares -Madrid):

- En la **Estación de Atocha (tren n° 21431)**, según la cinta de video del sistema de seguridad de la Estación de Atocha, a las 7 horas 37 minutos 47 segundos ya se había producido la primera explosión –originando que un gran número de viajeros se acumulase en las escaleras mecánicas situadas junto a la posición de la zona central del tren; a las 7 horas 38 minutos 36 segundos se produce la segunda explosión en el vagón 5, y a las 7 horas 38 minutos 40 segundos se produce la tercera explosión en el vagón 4 —el más cercano a las citadas escaleras mecánicas—; en total se produjeron TRES EXPLOSIONES de dichas características. Los artefactos estaban situados en los vagones 1, 4, 5 y 6 (sobre el artefacto localizado en el primer vagón del convoy, cabecera de tren, y que no estalló inicialmente, se realizaron maniobras para su desactivación por los equipos T.E.D.A.X del Cuerpo Nacional de Policía, explosionando a las 9 horas 59 minutos 18 segundos —según la cinta de video del sistema de seguridad; con posteridad, a las 10 horas 57 minutos 27 segundos se procede por los equipos T.E.D.A.X del C.N.P a realizar maniobras de desactivación sobre lo que consideraron un artefacto explosivo —que no resultó tal— en el vagón inmediato posterior al vagón cabecera del tren).
- A unos 800 metros de la **Estación de Atocha** (**tren n° 17305),** paralela la línea férrea a la Calle Téllez, sobre las 7 horas 39 minutos, se produjeron CUATRO EXPLOSIONES en los vagones 1, 4, 5 y 6 del tren, el cual, en el momento de las deflagraciones, estaba desplazándose a escasa velocidad por la línea ferroviaria.
- En la **Estación de El Pozo del Tío Raimundo (tren n° 21435)**, sobre las 7 horas 38 minutos, instantes después de iniciar la marcha (al apreciarse que la cabeza del tren tenía ligeramente rebasada la línea del semáforo) tuvieron lugar DOS EXPLOSIONES, en los vagones números 4 y 6 del tren. Los artefactos estaban situados en los pisos superiores de ambos vagones (asimismo fue localizado un tercer artefacto oculto en el interior de una mochila de color azul oscuro/negra que se hallaba en el andén de la parte derecha en la estación mencionada, a la altura del tercer vagón; sobre dicho artefacto se efectuaron maniobras de desactivación por los equipos T.E.D.A.X del C.N.P., explosionando finalmente el referido artefacto).

  En esta Estación se encontraba el artefacto explosivo que en la madrugada del día 12 de marzo de 2004 se localizó en la Comisaría de Distrito de Puente de Vallecas y se desactivó (tal y como con posterioridad se hará mención); el referido artefacto explosivo tenía marcado como hora de activación de la alarma-despertador las 7 horas 40 minutos.
- En la **Estación de Santa Eugenia (tren n° 21713)**, sobre las 7 horas 38 minutos tuvo lugar UNA EXPLOSIÓN en el 4° vagón del tren.

1.3. Los rastros de la investigación

El auto de procesamiento a que hacemos referencia, y que fue publicado por el diario español *El Mundo*, da cuenta de lo importante que resultó la evidencia digital. El rastreo de señales de teléfonos móviles, la revisión de su bitácora, el cruce de llamadas, la obtención oportuna tanto de órdenes de cateo como de intervención de equipos de cómputo, entre otras diligencias, permitieron dar con el paradero de los autores del atentado.

En la investigación se buscó no dejar nada al azar. La cronología de la investigación destaca:

2004
11 de marzo.- Una furgoneta robada es hallada, poco después de las explosiones, cerca de la estación de Alcalá de Henares, con siete detonadores, restos de explosivo y una cinta en árabe.
12 de marzo.- La policía desactiva un artefacto, escondido en una bolsa de deportes hallada en el

tren del Pozo del Tío Raimundo, compuesto de Goma 2 ECO, un detonador y un teléfono móvil, que fue la clave para la investigación.

La tarjeta del teléfono fue un punto de partida para detectar la bitácora de llamadas. A partir de éstas se hizo cruce de llamadas, revisión de otros números telefónicos móviles, hasta lograr la localización de los usuarios.

13 de marzo.- Siguiendo el rastro de la tarjeta hallada en el teléfono móvil, se producen las primeras detenciones —de tres ciudadanos marroquíes y dos indios—, entre ellas las de Jamal Zougam, finalmente procesado como presunto autor material de los atentados. Ese mismo día, un supuesto "portavoz militar" de Al Qaeda en Europa reivindica la masacre en un vídeo localizado cerca de la mezquita de la M-30.

18 de marzo.- Se producen nuevas detenciones, entre ellas las del ex minero José Emilio Suárez Trashorras, acusado de proporcionar los explosivos al comando autor de los atentados.

26 de marzo.- En una casa cercana a Morata de Tajuña (Madrid) se hallan detonadores, restos de explosivos y huellas dactilares de más de veinte personas.

2 de abril.- Es desactivada una bomba colocada en la vía del AVE Madrid-Sevilla en Mocejón (Toledo).

3 de abril.- Siete terroristas, cercados por la policía en un piso de Leganés, se suicidan activando los explosivos que tenían consigo.

15 de abril.- En una cinta sonora, el líder de Al Qaeda, Osama Bin Laden, reivindica implícitamente el 11-M y el 11-S: "es vuestra propia mercancía, que os ha sido devuelta".

27 de mayo.- El Parlamento crea una comisión para investigar el 11-M.

7 de junio.- Detenido en Milán (Italia) Rabei Osman El Sayed, "Mohamed el Egipcio", considerado autor intelectual de los atentados.

9 de junio.- Detenidos en Asturias otros seis miembros de la denominada "trama de los explosivos".

16 de noviembre.- Primer juicio por el 11-M. El menor G.M.V., "El Gitanillo", es condenado a seis años de internamiento en régimen cerrado por colaborar en el robo y traslado de los explosivos a Madrid.

17 de diciembre.- Detenido en Lanzarote el marroquí Hassan el Haski, presunto líder en España del Grupo Islámico Combatiente Marroquí (GICM), al que se atribuyen los atentados.

2005

1 de febrero.- Detenido en Bélgica Youssef Belhadj, considerado junto a "El Egipcio" y Hassan El Haski uno de los inductores de la masacre.

23 de julio.- Abdelmajid Bouchar "El Gamo", que logró escapar del cerco policial al piso de Leganés, es detenido en Serbia.

2006

11 de abril.- El juez Del Olmo dicta el procesamiento de 29 de los 116 imputados en el sumario, de ellos 15 marroquíes, nueve españoles, dos sirios, un egipcio, un argelino y un libanés.

16-19 de mayo.- El juez comunica el auto de procesamiento a los acusados, todos los cuales —salvo el español Sergio Álvarez— niegan las imputaciones.

7 de julio.- El juez Del Olmo concluye el sumario y eleva la causa a la sala de lo penal para su enjuiciamiento.

25 de septiembre.- La Audiencia Nacional confirma los 29 procesamientos y considera "perfectamente acreditado" que el explosivo fue Goma 2.

6 de noviembre.- La Fiscalía presenta su escrito de conclusiones provisionales, en el que solicita 270.885 años de cárcel para los 29 procesados.

La investigación en materia de evidencia digital fue no sólo efectiva, sino además, debidamente cuidada para ser llevada ante la Audiencia Nacional. Ese es el ejemplo que nos queda del caso que ahora referimos.

1.4. Clasificación de los ataques ciberterroristas

Jesús Edmundo Coronado Contreras establece que, los ataques ciberterroristas pueden clasificarse de la siguiente manera:

1. Simples: son los ataques orquestados contra sistemas en específico mediante herramientas creadas por otros. Son utilizados por grupos pequeños que no cuentan con grandes recursos y sus objetivos son menores.

2. Avanzados: son aquellos en los que organizaciones más estructuradas pueden atacar diversos sistemas y crear herramientas básicas para ello.
3. Complejos y coordinados: ataques ejecutados por organizaciones en contra de sistemas más sofisticados con herramientas propias y consecuencias mayores.

Dentro de los motivos que puede tener el terrorismo cibernético se encuentran:

1. Destruir la capacidad operacional del objetivo.
2. Destruir o afectar la reputación de una organización, país, etc.
3. Conseguir más seguidores y que los atacados cambien su afiliación.
4. Demostrar su poder tanto dentro de sus seguidores como dentro de sus objetivos.

Lo anterior encuentra en gran medida sustento en el atractivo de ejecutar ataques en el ciberespacio. En comparación con el terrorismo convencional, el "ciberterrorismo" permite que los terroristas causen un daño igual o mayor a su objetivo de una forma más económica y segura.

Dentro de los tipos de ataques ejecutados con propósitos terroristas podemos ubicar los siguientes:

1. Incursión: ataques con la intención de acceder en un sistema o red para obtener o modificar información.
2. Destrucción: al acceder a una red o sistema y destruir información puede conllevar a diversas consecuencias como daños económicos.
3. Desinformación: ataques que pueden tener consecuencias inmediatas, ya que al clonar páginas de Internet o usuarios dentro de una red se puede difundir información errónea y generar caos.
4. Denegación de servicio: ataque con el que se sobrecarga un servidor para que los usuarios (legítimos) no puedan tener acceso a los servicios prestados.[18]

De esta clasificación podemos arribar a la conclusión previa de que no todo ataque tiene como fin los establecidos en el Código Penal para el tipo de terrorismo, el fin es inutilizar equipos y no exactamente causar un temor en la población o bien perseguir algún fin último por parte del Estado (observar el punto número uno de esta clasificación, relativo a los ataques simples, los cuales parecen estar orientados a un sector de la economía).

1.5. Participación en el delito

Paulatinamente el grupo (obsérvese que se tiene la comisión del delito como una serie de pasos cometidos a través de la pluralidad de voluntades) que comete la conducta va migrando en estructura e intereses, que van desde el individual hasta el estatal, lo cual ya implica un nivel de responsabilidad que rebasa al Derecho penal tradicional, pues no se puede perseguir penalmente a un representante de un poder constituido, salvo lo relativo a la jurisdicción a que hace referencia el Estatuto de Roma y sólo para los delitos ahí contenidos.

1.6. Resultado material del delito

El ciberterrorismo va desde una mala entendida competencia desleal hasta una guerra en el campo virtual. La ciberguerra es el último paso en esta escalada, por lo que los bienes jurídicos tutelados que pueden afectarse son tan diversos, según la dimensión del ataque (puede tratarse de información, objetos, patrimonio, seguridad del Estado, la propia vida de las personas, etcétera).[19]

2. Problemas de la responsabilidad de las personas jurídicas y los aparatos organizados de poder

El ciberterrorismo puede realizarse, en materia de concurso de personas, tanto por un particular, como por

[18] "Breves consideraciones sobre la ciberdelincuencia y el ciberterrorismo". Consultado en http://www.ured.org.mx/ured/breves-consideraciones-sobre-la-ciberdelincuencia-y-el-ciberterrorismo/ 16 de abril de 2017; 17:49 h

[19] Pasos de un ciberataque

1. Investigación: recopilar y analizar la información existente acerca del blanco para identificar vulnerabilidades y decidir quiénes serán las víctimas.
2. Transporte: llegar al punto débil del sistema informático que se puede explotar. Suelen usarse estos métodos:
   Se crea un sitio web replicando a otro, que se ve prácticamente igual, y que la víctima usa con frecuencia.
   Se trata de acceder a los servicios en la red de la organización.
   Se envía un mail con un vínculo (link) a un sitio web malicioso o un archivo anexo infectado con algún virus.
   Se trata de infiltrar una memoria externa como un USB, por ejemplo.
3. Ingreso: explotar esa vulnerabilidad para obtener acceso no autorizado.
   Para lograrlo, se modifica el funcionamiento del sistema, se accede a las cuentas en la red, se obtiene el control de la computadora, el celular o la tableta del usuario.

una empresa y, en esa escalada, puede materializarse a través de los denominados aparatos organizados de poder, lo que de suyo implica una problemática bastante amplia.

La responsabilidad penal de las personas morales o jurídicas es sin duda un tema actual y por demás interesante, pero no exento de problemas como para considerarlo como un concepto totalmente acabado, y menos cuando se pueden cometer delitos trasfronterizos desde distintas latitudes y legislaciones aplicables, como por grupos de poder constituido. Es por ello, que la responsabilidad de las personas morales es un tema que debemos acotar, por lo menos en la teoría para conocer su significado y alcance en la práctica.

La discusión sobre la responsabilidad penal de las personas morales ha sido un tema polémico entre aquellas generaciones que postularon que sólo las personas físicas son penalmente responsables, y la nueva generación de autores que ven en la constitución de las personas jurídicas un boquete de impunidad que debe ser resuelto con esta nueva postura.

Durante mucho tiempo la doctrina dominante señaló tajantemente que las personas morales no delinquen (y así se estableció en el Código Penal para el Distrito Federal de 2002, en su artículo 27), pero algo quedó en el tintero, porque la discusión no se apagó.

Hace algunos años, el doctor Fernando Flores García escribió unas líneas extraordinarias, cuando el tema no cobraba la vigencia que tiene hoy. En la conclusión de su análisis el extraordinario maestro escribió:

> Se han logrado considerables avances y establecido puntos de coincidencia. Es de desearse que en futuros congresos jurídicos, en libros, ensayos, proyectos legislativos, etc., se renueven los esfuerzos para dar una solución que resuelva los problemas que en la vida real representan las actividades ilícitas de las personas jurídicas colectivas. [20]

¡Con cuánta anticipación dejó esas líneas para ser desarrolladas casi treinta años después!

Y es que al hablar de responsabilidad debe quedar claro si el concepto parte de la sustitución del juicio de reproche, o bien es la consecuencia procesal de un acto en particular.

En todo caso, la voluntariedad y conocimiento que exige la culpabilidad, siempre serán un gran reto para quien diserte sobre este tema.

Recientemente se han desarrollado distintas iniciativas de ley, derivadas de los instrumentos internacionales que ha firmado México, entre los cuales destacan la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y la Convención de las Naciones Unidas contra la Corrupción que contienen la posibilidad de que los Estados legislen sobre la responsabilidad penal de las personas jurídicas.

La Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional en su artículo 10 señala:

> **Artículo 10. Responsabilidad de las personas jurídicas**
>
> 1. Cada Estado Parte adoptará las medidas que sean necesarias, de conformidad con sus principios jurídicos, a fin de establecer **la responsabilidad de personas jurídicas** por participación en delitos graves en que esté involucrado un grupo delictivo organizado, así como por los delitos tipificados con arreglo a los artículos 5, 6, 8 y 23 de la presente Convención.
>
> 2. Con sujeción a los principios jurídicos del Estado Parte, **la responsabilidad de las personas jurídicas podrá ser de índole penal**, civil o administrativa.
>
> **3. Dicha responsabilidad existirá sin perjuicio de la responsabilidad penal que incumba a las personas naturales que hayan perpetrado los delitos.**
>
> 4. **Cada Estado Parte velará en particular porque se impongan sanciones penales** o no penales eficaces, proporcionadas y disuasivas, incluidas sanciones monetarias, a las personas jurídicas consideradas responsables con arreglo al presente artículo.

Por su parte, la Convención de las Naciones Unidas contra la Corrupción establece lo siguiente:

---

4. Afectar: realizar actividades dentro del sistema para lograr lo que el hacker quiere. *(BBC Mundo)* http://www.insightmx.com.mx/detallenota.php?id_news=125 consultado el 16 de abril de 2017; 17:30 hs.

[20] Véase Flores García, Fernando, "La responsabilidad penal de la persona jurídica colectiva", en *Ensayos jurídicos*, Facultad de Derecho (Cincuentenario de la Revista de la Facultad de Derecho de México), UNAM, 1989, pp. 99-143. Véase también: Flores García, Fernando, "Principales Corrientes acerca de la Responsabilidad Penal de la Persona Jurídica Colectiva", en *Liber Ad Honorem Sergio García Ramírez*, Tomo II, UNAM, Instituto de Investigaciones Jurídicas, México, 1998.

Artículo 26. Responsabilidad de las personas jurídicas

1. Cada Estado Parte adoptará las medidas que sean necesarias, en consonancia con sus principios jurídicos, a fin de **establecer la responsabilidad de personas jurídicas por su participación en delitos tipificados con arreglo a la presente Convención.**

2. Con sujeción a los principios jurídicos del Estado Parte, **la responsabilidad de las personas jurídicas podrá ser de índole penal**, civil o administrativa.

3. Dicha responsabilidad existirá sin perjuicio de la responsabilidad penal que incumba a las personas naturales que hayan cometido los delitos.

4. **Cada Estado Parte velará en particular por que se impongan sanciones penales** o no penales eficaces, proporcionadas y disuasivas, incluidas sanciones monetarias, a las personas jurídicas consideradas responsables con arreglo al presente artículo.

Asimismo, en el ámbito nacional se han abordado en varias iniciativas de ley lo relativo a la responsabilidad de las personas morales, con distintas perspectivas doctrinales, y diferentes soluciones. Además se ha abonado lo relativo a los derechos humanos que le son propios a las personas jurídicas,[21] sin embargo, de la lectura de los pocos artículos que le dedica al tema el Código Nacional de Procedimientos Penales (artículos 421 al 425), podemos vislumbrar que el procedimiento penal a las personas jurídicas apenas está en sus comienzos.[22]

3. La reforma al Código Penal para el Distrito Federal

El 22 de diciembre de 2014 se publicó en la *Gaceta del Distrito Federal* (hot Ciudad de México) el Decreto por el que se reforman, adicionan y derogan diversos artículos del Código Penal para el Distrito Federal que establece un breve capítulo sobre un tema ingente que produce más dudas sobre su aplicación, puesto que el ciberterrorismo puede provenir de órganos de algún Estado (extranjero), lo que implica otra clase de responsabilidad internacional.[23]

En pocas palabras, la mayor parte de lo establecido para las personas morales podría no ser válido tratándose de órganos de poder en el extranjero que fomentan esta clase de actos. Es claro que si para los

---

[21] "Las personas morales gozan de aquellos derechos fundamentales que conforme a su naturaleza le resulten necesarios para la realización de sus fines con el fin de proteger su existencia, su identidad y asegurar el libre desarrollo de su actividad". Así lo estableció el Pleno de la Suprema Corte de Justicia de la Nación el 21 de abril de 2014, al resolver la Contradicción de Tesis 360/2013.

[22] Ramón Eduardo Ribas escribe sobre el el procedimiento penal a las personas jurídicas: "La construcción de un sistema de responsabilidad penal de las personas morales puede encauzarse jurídicamente a través de dos vías fundamentales:

a) En primer lugar, acudiendo a las categorías y criterios de imputación penales ya conocidos.

b) Creando, en segundo término, un nuevo Derecho Penal, exclusivo de las entidades colectivas.

La primera de estas soluciones consiste en *adoptar* el Derecho Penal clásico, de base individualista, y aplicarlo a los comportamientos criminales protagonizados por entidades colectivas. Obviamente, dicha adopción y la subsiguiente aplicación no pueden realizarse de forma mecánica o automática; sería preciso ajustar, antes, mediante una reinterpretación funcionalista, la teoría del delito individual. Sin esta nueva normativización de los conceptos penales, la inadecuación de éstos para enfrentarse a formas de criminalidad colectiva obligaría a una *resignación descriptiva* o a crear un sistema de responsabilidad penal específico para empresas o personas colectivas. Característico de estos planteamientos es, en fin, su intento de adecuar las categorías penales a las personas jurídicas antes que sustituirlas por otras.

Radicalmente contraria a la flexibilización de las categorías penales existentes, se muestra Zúñiga Rodríguez. En su opinión, dicha flexibilización comportaría el riesgo de "contaminar" todo el sistema de responsabilidad individual pudiendo desembocar en la pérdida de la validez de las garantías ganadas y construidas durante dos siglos. También Tamarit Sumalia considera, ante los riesgos de «contaminación conceptual» que pudieran derivarse de la integración de la responsabilidad de las personas jurídicas en el sistema penal, sería aconsejable un "dualismo no disgregador del sistema".

La segunda solución, a mi juicio más plausible, toma como punto de partida la siguiente idea: las personas jurídicas, por ser sujetos diferentes, necesitan de un derecho penal distinto del de las personas físicas, precisamente porque el problemas es que éste no les resulta aplicable. Asumida la necesidad de un Derecho Penal distinto, será necesario determinar qué deberá tener este nuevo Derecho *antiguo* para seguir conceptuándolo como Penal: si no tuviera nada, no nos hallaríamos ante un Derecho Penal distinto, sino, como indica García Arán, ante algo distinto del Derecho Penal". (Ribas, Ramón Eduardo, *La persona jurídica en el Derecho penal. Responsabilidad civil y criminal de la empresa*, Editorial Comares, Granada, 2009, pp. 281 – 282).

[23] **La responsabilidad penal desde el seno de la persona moral.-**

ARTÍCULO 27 (Responsabilidad penal en el seno de una persona moral o jurídica). Quien actúe:

a).- Como administrador de hecho de una persona moral o jurídica;

b).- Como administrador de derecho de una persona moral o jurídica, o

c).- En nombre o representación legal o voluntaria de otra persona.

Y en estas circunstancias cometa un hecho que la ley señale como delito, responderá personal y penalmente, aunque no concurran en él las condiciones, cualidades o relaciones que el tipo penal requiera para poder ser sujeto activo del mismo, si tales circunstancias sí concurren en la entidad o persona en cuyo nombre o representación se actúa.

delitos cometidos por un particular desde el extranjero se requiere de una amplia colaboración internacional, en los casos de empresas y gobiernos, estamos apenas observando la punta del iceberg del problema.

4. Conclusiones

El ciberterrorismo debe entenderse como el terrorismo por medios electrónicos o informáticos.

No está contemplado el medio comisivo no violento (electrónico) en el tipo penal de terrorismo establecido en el Código Penal federal.

El ciberterrorismo puede afectar de manera contundente a la economía no sólo de una persona o industria, sino el correcto funcionamiento de la economía de un país, motivo por el cual debe ser observado como un riesgo que debe atenderse con programas de corto y mediano plazo.

El ciberterrorismo puede ser cometido por una o más personas, debe agravarse la comisión por un grupo o empresa y deben buscarse soluciones para cuando esta conducta es alentada, permitida, patrocinada o ejecutada por un Estado.

El ciberterrorismo es la antesala de la ciberguerra.

5. Bibliografía

Cano Paños, Miguel Ángel, "El binomio internet/terrorismo islamista", en *Iter Criminis,* año 4, número 21, Inacipe, mayo-junio 2011.

Se entenderá por administrador, la persona que realiza actos de administración en una persona moral o jurídica, sea cual fuere el nombre o denominación que reciba conforme a las leyes aplicables o según la naturaleza jurídica del acto por el cual así se asuma.

La responsabilidad penal de la persona moral.-

Artículo 27 Bis (Responsabilidad Penal de una Persona Moral o Jurídica).

I.- Las personas morales o jurídicas serán responsables penalmente de los delitos dolosos o culposos, y en su caso, de la tentativa de los primeros, todos previstos en este Código, y en las leyes especiales del fuero común, cuando:

a) Sean cometidos en su nombre, por su cuenta, en su provecho o exclusivo beneficio, por sus representantes legales y/o administradores de hecho o de derecho; o

b) Las personas sometidas a la autoridad de las personas físicas mencionadas en el inciso anterior, realicen un hecho que la ley señale como delito por no haberse ejercido sobre ellas el debido control que corresponda al ámbito organizacional que deba atenderse según las circunstancias del caso, y la conducta se realice con motivo de actividades sociales, por cuenta, provecho o exclusivo beneficio de la persona moral o jurídica;

Cuando la empresa, organización, grupo o cualquier otra clase de entidad o agrupación de personas no queden incluidas en los incisos a) y b) de este artículo, por carecer de personalidad jurídica y hubiesen cometido un delito en el seno, con la colaboración, a través o por medio de la persona moral o jurídica, el Juez o Tribunal podrá aplicarles las sanciones previstas en las fracciones I, III, V, VI, VII, y IX del artículo 32 de este Código.

Quedan exceptuados de la responsabilidad de la persona moral o jurídica, las instituciones estatales, pero cuando aquélla utilice a éstas últimas para cometer un delito será sancionada por el delito o delitos cometidos. Lo anterior también será aplicable a los fundadores, administradores o representantes que se aprovechen de alguna institución estatal para eludir alguna responsabilidad penal.

Principio de proporcionalidad aplicable a las personas morales

Artículo 27 Ter.- En caso de que se imponga la sanción de multa por la comisión de un delito, tanto a la persona física como a la persona moral o jurídica, el juez deberá observar el principio de proporcionalidad para la imposición de las sanciones.

Hipótesis de no exclusión de responsabilidad de las personas morales

Artículo 27 Quáter.- No excluirá ni modificará la responsabilidad penal de las personas morales o jurídicas:

I.- Que en las personas físicas mencionadas en el artículo 27 bis, concurra alguna de las siguientes circunstancias:

a).- Una causa de atipicidad o de justificación;

b).- Alguna circunstancia que agrave su responsabilidad;

c).- Que las personas hayan fallecido; o

d).- Que las personas se hubiesen sustraído a la acción de la justicia.

II.- Que en la persona moral o jurídica concurra:

a).- La transformación, fusión, absorción, escisión de la persona moral o jurídica, la que será trasladable a la entidad en que se transforme, se fusione, se absorba o se escinda.

El Juez o el Tribunal podrán anular la transformación, fusión, absorción o escisión de la persona moral o jurídica, con el fin de que los hechos no queden impunes y pueda imponerse la sanción que corresponda. No será necesaria la anulación cuando la sanción consista en multa.

En caso de que la transformación, fusión, absorción o escisión constituya delito diverso al que se está sancionando a la persona moral o jurídica, el Juez o Tribunal deberá aplicar las reglas que del concurso prevé este Código y demás ordenamientos jurídicos aplicables; o

b).- La disolución aparente.

Se considerará que existe disolución aparente de la persona moral o jurídica, cuando ésta continúe su actividad económica y se mantenga la identidad sustancial de clientes, proveedores y empleados, o de la parte más relevante de todos ellos.

CAPÍTULO XIII

SUSPENSIÓN, DISOLUCIÓN, PROHIBICIÓN DE REALIZAR DETERMINADOS NEGOCIOS, OPERACIONES O ACTIVIDADES, REMOCIÓN, INTERVENCIÓN, CLAUSURA, RETIRO DE MOBILIARIO URBANO, CUSTODIA O RESGUARDO DE FOLIOS, INHABILITACIÓN Y REPARACIÓN DEL DAÑO DE LAS PERSONAS MORALES O JURÍDICAS

Conway, Maura, "*Cyberterrorism: The Story So Far"* Department of Political Science 1, Trinity College, Dublin, Ireland, 2013. Disponible en: http://doras.dcu.ie/496/1/info_warfare_2_2_2003.pdf

Guibourg, Ricardo A., *Informática Jurídica Decisoria*, Astrea, Buenos Aires, 1993.

Hargreaves C. y D. Prince, "*Understanding cyber criminals and measuring their future activity developing cybercrime research"*, Security Lancaster, Lancaster University. Disponible en: http://eprints.lancs.ac.uk/65477/1/Final_version_Understanding_cyber_criminals_and_measuring_their_activity.pdf

Jalil S.A., *Countering Cyber Terrorism Effectively: Are We Ready To Rumble?* GIAC Security Essentials Certification (GSEC) Practical Assignment, Version 1.4b, Option 1, junio 2003. Disponible en: http://www.giac.org/paper/gsec/3108/countering-cyber-terrorism-effectively-ready-rumble/105154

Koops, Bert-Jaap, *The Internet and its Opportunities for Cybercrime,* 2010.

Lessig, Lawrence., *Code and other Laws of cyberspace,* Basic books, U.S.A, 1999.

Pollitt, Mark citado por Krasavin, S. *What is Cyberterrorism?* Computer Crime Research Centre. Disponible en: http://www.crime-research.org/library/Cyber-terrorism.htm

Porte Petit Candaudap, Celestino, *Programa de Derecho Penal, Parte General,* 3ª ed. Trillas, México, 1990.

Luciano Salellas, "Delitos Informáticos, Ciberterrorismo, V.1.201". *Boletín Informativo de Seguridad* (http://www.cabinas.net/monografias/informatica/delitos_informativos_ciberterrorismo.pdf).

Alcances de las consecuencias jurídicas para las personas morales

ARTÍCULO 68 (Alcances y duración de las consecuencias para las personas morales). La suspensión consistirá en la cesación de la actividad de la persona moral o jurídica durante el tiempo que determine el Juez en la sentencia, la cual no podrá exceder de cinco años.

La disolución consistirá en la conclusión definitiva de toda actividad social de la persona moral o jurídica, que no podrá volverse a constituir por las mismas personas en forma real o encubierta. La conclusión de toda actividad social se hará sin perjuicio de la realización de los actos necesarios para la disolución y liquidación total. El Juez designará en el mismo acto un liquidador que procederá a cumplir todas las obligaciones contraídas hasta entonces por la persona moral o jurídica, inclusive las responsabilidades derivadas del delito cometido, observando las disposiciones legales sobre prelación de créditos, conforme a la naturaleza de éstos y de la entidad objeto de la liquidación.

La prohibición de realizar determinados negocios, operaciones o actividades, se referirá exclusivamente a las que determine el juzgador, mismas que deberán tener relación directa con el delito cometido. La prohibición podrá ser definitiva o temporal, en este último caso, el juez podrá imponerla hasta por cinco años. Los administradores y el comisario de la sociedad serán responsables ante el Juez, del cumplimiento de esta prohibición e incurrirán en las penas que establece este Código por desobediencia a un mandato de autoridad.

La remoción consiste en la sustitución de los administradores por uno designado por el juez, durante un período máximo de cinco años.

…

…

La intervención consiste en la vigilancia de las funciones que realizan los órganos de representación de la persona moral o jurídica y se ejercerá con las atribuciones que la ley confiere al interventor, hasta por tres años.

La clausura consistirá en el cierre de todos o algunos de los locales o establecimientos de la persona moral o jurídica por un plazo de hasta cinco años.

La inhabilitación consiste en la falta de capacidad para obtener subvenciones y ayudas públicas, para contratar con el sector público y para gozar de beneficios e incentivos fiscales o de seguridad social, por un plazo de hasta quince años.

Para la aplicación de la reparación del daño, se estará a lo previsto en este Código y el juez podrá establecer como garantía para la misma, el otorgamiento de billete de depósito, una cantidad en efectivo o cualquiera otra medida a satisfacción de la víctima u ofendido del delito.

El retiro de mobiliario urbano, incluidas casetas telefónicas o parte de ellas, cuando éstos no hayan sido removidos por otra autoridad, consiste en la remoción que realice personal de cualquier institución de seguridad pública por orden del juez. El mobiliario urbano quedará en resguardo del área que corresponda de la Procuraduría General de Justicia del Distrito Federal.

Para la custodia del folio real o de persona moral o jurídica se estará a lo dispuesto en la Ley Registral para el Distrito Federal, su reglamento y demás ordenamientos jurídicos aplicables.

Prelación de derechos sobre las personas morales sancionadas

ARTÍCULO 69. Al imponer las consecuencias jurídicas accesorias previstas en este Capítulo, el Juez tomará las medidas pertinentes para dejar a salvo los derechos de los trabajadores y terceros frente a la persona jurídica colectiva, así como aquellos otros derechos que sean exigibles frente a otras personas, derivados de actos celebrados con la persona moral o jurídica sancionada.

Estos derechos quedan a salvo, aun cuando el juez no tome las medidas a que se refiere el párrafo anterior.

Individualización de las sanciones para personas morales

ARTÍCULO 72 bis (Criterios para la individualización de las penas y medidas de seguridad para las personas morales o jurídicas). El Juez, para la imposición de las penas y medidas de seguridad previstas en el artículo 32, 38, 68 y 69 de este Código, tomará en cuenta:

I. La naturaleza de la acción u omisión y los medios empleados para ejecutarla;

II. La magnitud del daño causado al bien jurídico o del peligro en que éste fue colocado;

III. Las circunstancias de tiempo, lugar, modo y ocasión del hecho realizado;

IV.- El beneficio obtenido por la comisión del delito;

V.- Lo previsto en los artículos 42, y 43 de este Código y demás artículos aplicables;

Vasconcelos Santillán, Jorge, *Informática I, Computación Básica*, Publicaciones Cultural, México, 2002.

6. Fuentes electrónicas

http://www.insightmx.com.mx/detallenota.php?id_news=125 consultado el 16 de abril de 2017; 17:30 hs.

http://www.webopedia.com/TERM/c/cyberspace.html

http://www.ured.org.mx/ured/breves-consideraciones-sobre-la-ciberdelincuencia-y-el-ciberterrorismo/

http://www.policia.cl/paginas/brigadas/bg-bricib/bg-bricib.htm

http://www.policiaiformatica.gob.pe/nosotros.asp

http://www.insightmx.com.mx/detallenota.php?id_news=125

VI.- La necesidad de prevenir y evitar la continuidad de la actividad delictiva o de sus efectos;

VII.- Las consecuencias económicas, sociales, y en su caso, las repercusiones para los trabajadores; y

VIII.- El puesto o cargo que en la estructura de la persona moral o jurídica ocupa la persona física u órgano que cometió el delito y/o incumplió con el deber de control.

Tentativa para las personas morales

ARTÍCULO 78 (Punibilidad de la tentativa)…

…

Este artículo será aplicable para los casos en que la persona moral o jurídica incurra en una tentativa.

Asociación delictuosa y persona moral

ARTÍCULO 192. Las sanciones que se señalan en el Título Sexto, del Libro Segundo, se triplicarán, cuando el delito sea cometido por una asociación delictuosa.

Cuando una o más de las conductas descritas en el presente Título resulte cometida a nombre, bajo el amparo o a beneficio de una persona moral o jurídica, a ésta se le impondrán las consecuencia jurídicas consistentes en clausura, disolución y multa hasta por 1,500 días multa, independientemente de la responsabilidad en que hubieren incurrido las personas físicas por el delito cometido.