Ciberterrorismo. Regulación y estrategias para combatirlo

PID_00272606

Josep Maria Tamarit Sumalla
Nasserine Montornés Mataoui
Ma. del Carme Guirao Cid

Tiempo mínimo de dedicación recomendado: 3 horas

Universitat Oberta de Catalunya

Josep Maria Tamarit Sumalla

Catedrático de Derecho penal en la Universitat Oberta de Catalunya, donde es director del Máster en Ciberdelincuencia. Su actividad de investigación se ha centrado básicamente en aspectos relacionados con la victimología, la justicia restaurativa y el sistema de sanciones penales. Tiene también varias publicaciones relacionadas con la delincuencia de motivación ideológica y los delitos de odio. Es coordinador del Grupo consolidado de investigación sobre el Sistema de justicia penal.

Nasserine Montornés Mataoui

Graduada en Criminología por la UOC y Máster en Sistema de Justicia Penal en la Universitat de Lleida. Se está formando en el Instituto de Seguridad Pública de Cataluña y es tutora del Máster en Ciberdelincuencia de la UOC.

Ma. del Carme Guirao Cid

Graduada en Criminología por la UOC y Máster en Derechos Humanos por la misma Universidad. Es becaria predoctoral en la Universitat de Lleida, donde realiza su tesis doctoral sobre adoctrinamiento y victimización terrorista, tema respecto al cual ha publicado dos artículos (2018; 2019).

El encargo y la creación de este recurso de aprendizaje UOC han sido coordinados por el profesor: Josep Maria Tamarit Sumalla (2020)

Primera edición: febrero 2020

Av. Tibidabo, 39-43, 08035 Barcelona
Realización editorial: FUOC

Índice

Introducción

El ciberterrorismo se ha convertido en una de las principales preocupaciones para la comunidad internacional. Con el uso de las herramientas cibernéticas los patrones de conducta de los terroristas son cada vez más difíciles de predecir, al poder desarrollar sus acciones en cualquiera de los ilimitados ámbitos del ciberespacio. A continuación haremos referencias a la *Deep Web* y a la *Dark Net*, poniendo especial énfasis en el sistema TOR (The Onion Router) por ser el más utilizado por parte de las organizaciones terroristas, ya que permiten a sus usuarios actuar bajo el anonimato.

La mayor inseguridad que genera el ciberterrorismo se debe a su elevada capacidad para adaptarse a nuevos contextos (incluidos los cibernéticos), y por el hecho de disponer de sistemas informáticos lo suficientemente desarrollados para penetrar en los sistemas de seguridad estatales o institucionales, lo que produce un daño considerable. Dada la inseguridad que generan sus acciones, el ciberterrorismo tiene cada vez mayor protagonismo en las agendas políticas de los distintos Estados. Sin embargo, del mismo modo que ocurría con la definición de ciberterrorismo, actualmente no existe ningún instrumento legal que haya adquirido el consenso necesario para que el uso malintencionado de internet por parte de las organizaciones terroristas acabe siendo castigado a través de un único tipo. Por este motivo, la regulación jurídica del terrorismo ha tendido a desarrollarse desde un ámbito nacional y pensando en el terrorismo *offline*. No obstante, el contenido de las normas penales ha ido modificándose cada vez que se ha producido un nuevo atentado, y varias veces han sido fuertemente criticadas al considerar que algunos de sus artículos violan determinados derechos y libertades fundamentales, siendo los relativos a la libertad de expresión los más perjudicados.

A nivel internacional, una ley antiterrorista que marcó un hito fue la USA Patriot Act (*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism*). Tras los atentados del 11S, Estados Unidos adoptó con esta nueva normativa una serie de medidas destinadas a restringir derechos y libertades bajo el pretexto de la seguridad. A partir de ella, queda permitido a las autoridades perseguir, capturar, encarcelar e interrogar a sospechosos de terrorismo en todo el mundo, escuchar las comunicaciones sin intervención judicial y negar la entrada al país a individuos sospechosos de pertenecer a una organización terrorista, entre otros. Con el fin de suavizar estas restricciones sobre las libertades individuales, en 2015 dicha ley fue substituida por la USA Freedom Act, que afectó, principalmente, a la gestión y almacenamiento de información y datos de los ciudadanos estadounidenses por parte de los servicios de inteligencia. Posteriormente, a modo de reflejo, han ido surgiendo otras leyes en otros países, como, la ley antiterrorista francesa que impulsó François Hollande tras la oleada de atentados que tuvieron lugar

en la capital parisina en noviembre de 2015. Esta concedió amplios poderes al Ministerio del Interior, tales como realizar registros domiciliarios basados en meras sospechas y sin necesidad de una orden judicial previa, arrestos domiciliarios, y la obligación de presentarse diariamente en comisaría. Todo ello fue consecuencia del estado de excepción que duró hasta finales de 2017, cuando una nueva mayoría parlamentaria, bajo la presidencia de Emmanuel Macron, aprobó una nueva ley que lo canceló. No obstante, se mantienen algunos de los aspectos más criticados, como la limitación de movimiento, la potestad policial de realizar registros sin orden judicial (aunque limita su ejecución de 6 de la mañana a 21 horas de la noche) o la facultad gubernamental para cerrar aquellos lugares de culto donde sospeche que se expongan ideas o lancen mensajes que alimenten la violencia.

Estas no fueron las únicas iniciativas polémicas. En el ámbito de la Unión Europea destaca la Directiva de 21 de abril de 2016 aprobada por el Parlamento Europeo con el objetivo de crear un registro de nombres de pasajeros aéreos (Passenger Name Record o PRN) como una herramienta más en la lucha antiterrorista, partiendo del hecho de que las actividades terroristas (y de delincuencia organizada) conllevan desplazamientos internacionales. Dado que dentro del espacio Schengen no existe restricción de movimiento para los ciudadanos de los Estados miembros, la Directiva estableció poder llevar a cabo un control e intercambio entre autoridades policiales sobre los datos de los pasajeros de las aerolíneas. En total, el PRN recopila hasta 19 variables de información sobre el pasajero, como itinerario, nombre y datos de contacto, detalles de pago, agencia de viajes, equipaje y número de asiento, entre otras. Todas estas iniciativas serán examinadas a lo largo de las siguientes páginas apoyándonos en gran medida en los puntos II, III y IV del documento de la UNODC, ***El uso de internet con fines terroristas***.

Objetivos

Los objetivos que se pretende conseguir al concluir el estudio del presente módulo sobre regulación y estrategias para combatir el ciberterrorismo son:

1. Conocer la vinculación de la *Deep Web* y la *Dark Web* con el ciberterrorismo.

2. Conocer el sistema TOR y su importante papel en el ciberterrorismo.

3. Conocer la evolución de la legislación antiterrorista a nivel internacional.

4. Describir el contenido de las principales leyes antiterroristas en España y su aplicación al campo del ciberterrorismo.

5. Conocer las principales estrategias desarrolladas para hacer frente al ciberterrorismo.

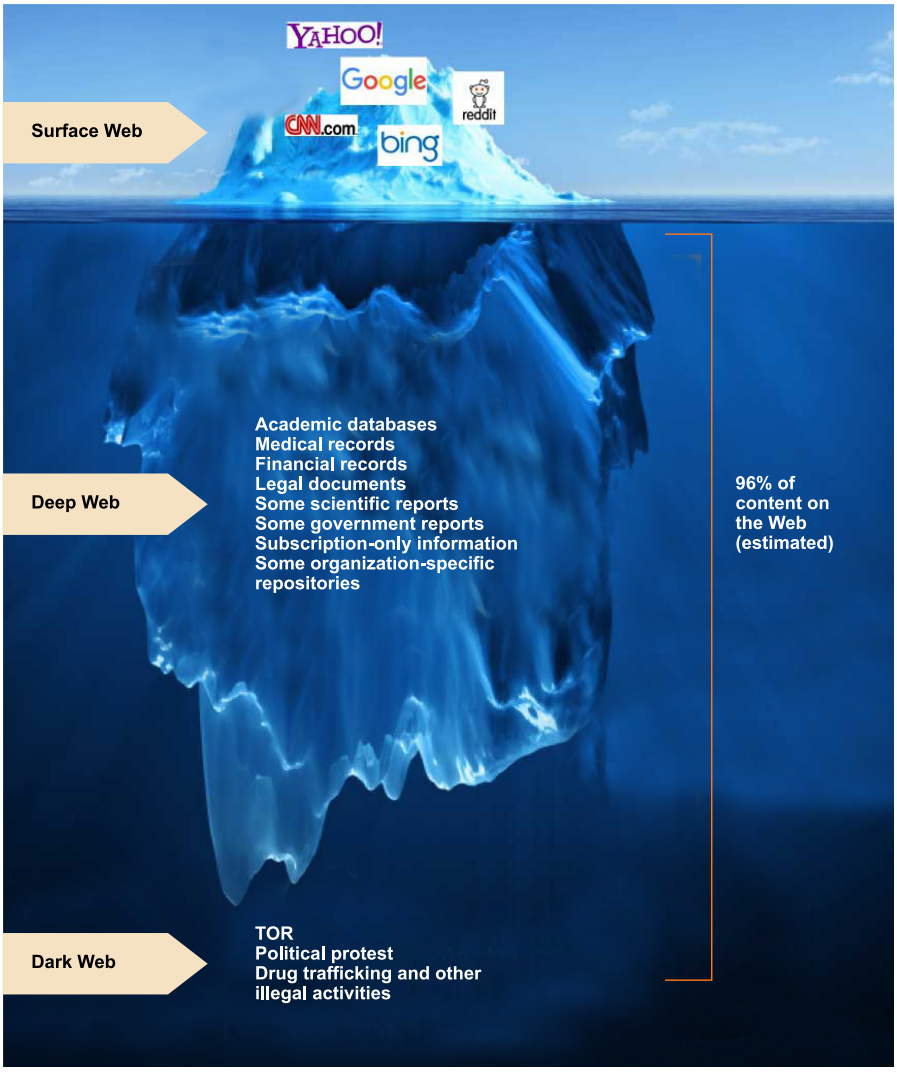
1. Las diversas capas de internet

Cuando navegamos por internet, a través del navegador Google o Yahoo la mayoría de veces, es probable que pensemos que todo está ahí y que lo podemos consultar en apenas unos segundos. Sin embargo, esto no es así. Lo que vemos (o mejor dicho, a lo que accedemos) es la *clear net* o *surface net*. El ciberespacio que consultamos en nuestro día a día solo representa una mínima parte de la realidad que en él se alberga, ya que mucho material queda oculto. Solamente aquellas personas con el conocimiento adecuado pueden sumergirse y explorar el fondo de la red. Entre ellas están los miembros de organizaciones terroristas. Sin embargo, hemos de aclarar que el espacio profundo de la red no solo se utiliza para fines ilícitos como la compra y venta de armas o drogas o el intercambio de material pornográfico, pues pueden realizarse otras muchas actividades con otra clase de finalidades.

1.1. Definición y delimitación de conceptos

El ciberespacio que existe más allá de navegadores como Google o Firefox es lo que se conoce como internet profunda o red oscura (por sus nombres en inglés *Deep Web* y *Dark Web*). A esta fracción de ciberespacio no podemos acceder a través de buscadores habituales, dado que se requieren unas determinadas plataformas para llegar a ella. Este es el principal motivo por el cual estos espacios resultan muy atractivos para los terroristas y para cometer delitos en general. Según estudiamos en el primer módulo, una de las características que definían el ciberespacio era el anonimato, y precisamente estas herramientas lo garantizan. Su uso no deja rastro susceptible de ser detectado, a priori, por los cuerpos y fuerzas de seguridad. A continuación vamos a entrar en las profundidades de la red para tomar conciencia de que existe ciberactividad más allá de la *clear net*. Además, creemos que el contenido de este apartado puede ser más provechoso de cara al estudio si presentamos las distintas capas o niveles de la red bajo la «metáfora del iceberg», dado que el material que nosotros consultamos es una ínfima parte de la extensión real del ciberespacio, quedando oculto el 96 %, aproximadamente, de su contenido.

Figura 1. Los diferentes niveles de internet según la figura de un iceberg



1.2. Deep Web

El término *Deep Web* (o internet profunda) fue utilizado por primera vez por Mike K. Bergman cuando se percató de que realizar una búsqueda por internet podía ser algo más complicado de lo que indicaba la apariencia y que incluía otros espacios que no eran visibles o accesibles para la mayoría de los usuarios. Estas conclusiones derivaban de un estudio que realizó en 2001 en el que comprobó que la *clear net* contenía 19 terabytes (TB) de información, mientras que la *Deep Web* era de 7.500, lo que evidenciaba que en esta ubicación la información existente era, aproximadamente, 400 veces superior (Bergman, 2001).

A la *Deep Web* se le suele atribuir connotaciones peyorativas, dada la creencia mayoritariamente compartida que defiende que en ella se realizan todo tipo de actividades ilegales como, por ejemplo, la compraventa de materiales ilícitos, intercambio de material pornográfico, etc. Sin embargo, esto no es así. La *Deep Web* alberga mayoritariamente contenido sensible referente a los ciudadanos, por ejemplo, datos médicos, números bancarios, infracciones administrativas o penales, etc. Del mismo modo, nosotros, cuando utilizamos aplicaciones co-

mo Dropbox o Google Drive para guardar o compartir documentos, fotos o vídeos también estamos utilizando esta capa de internet. Fijémonos que para poder acceder a ellas nos piden claves de seguridad que nos redirigen automáticamente a otros servidores. Por lo tanto, definiremos la *Deep Web* como:

> Parte de la web que subyace a la *clear net*, cuyo contenido no está indexado por motores de búsqueda convencionales o más utilizados, y que está protegido por claves de seguridad, dificultándose su rastreo.

1.3. Dark Web y Dark Net

La *Dark Net* (o red oscura) es el nivel último que hemos presentado a través del gráfico del iceberg y forma parte de la *Deep Web*. No obstante, a diferencia de esta, para acceder a la *Dark Web* no se requiere solamente un código de seguridad, sino unos navegadores determinados, siendo TOR el más utilizado por ciberdelincuentes, incluidas las organizaciones terroristas. Además de este también existen otros como IP2, ZeroNet o Freenet.

DuckDuckGo

DuckDuckGo (DDG) es un buscador similar a Google, desarrollado en Pensilvania por Gabriel Weinberg (Estados Unidos), pero que a diferencia de los existentes garantiza al usuario su privacidad. Es decir, la actividad que podamos llevar a cabo en ellas no queda registrada. Por este motivo, año tras año, va ganando popularidad frente a otros motores de búsqueda como los anteriormente citados. Por otro lado, cuando hablamos de **The Hidden Wiki** hacemos referencia al directorio de sitios webs que operan bajo el dominio «.onion» cuyo contenido puede ser editado de forma anónima por cualquier persona. Como os habréis percatado, se trata de una estructura que opera de forma similar a como lo hace la Wikipedia.

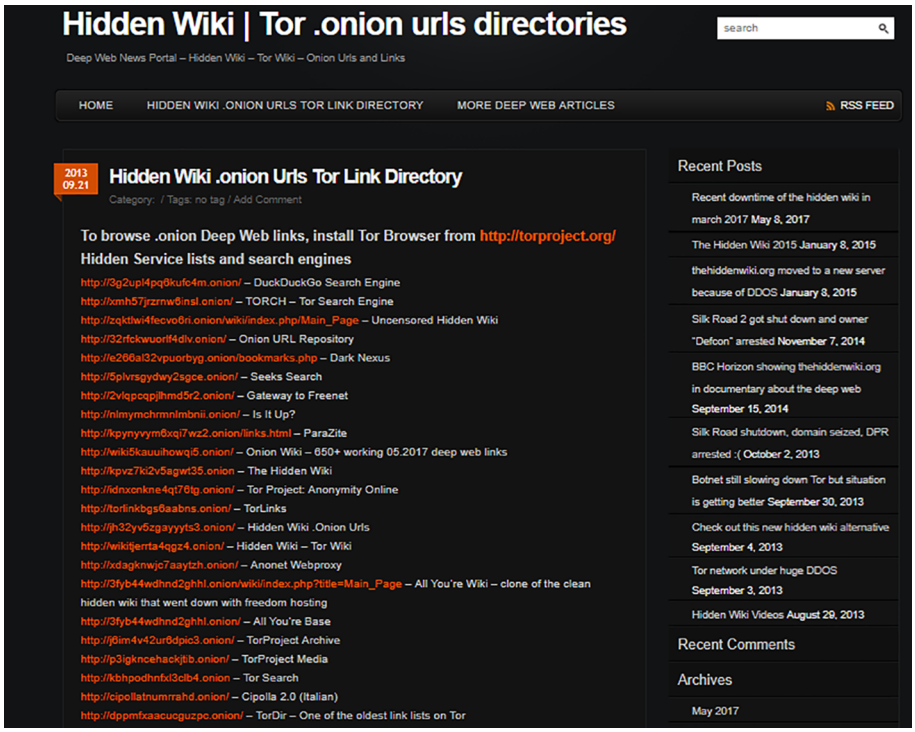
Como hemos mencionado al inicio, TOR es la abreviatura de The Onion Router, un proyecto que se inició con el objetivo de crear una red de comunicaciones paralela, y de nivel superior, al internet popularmente concebido, de manera que nunca se pudieran conocer los datos de sus usuarios, manteniéndose, así, como una red privada y anónima. Esto se consigue al no usar una red P2P («*peer to peer*», o de igual a igual), como sí utilizan los motores de búsqueda convencionales. Esto permite al usuario poder acceder, consultar o enviar información por vías independientes de la *clear net*. Sin embargo, esto no significa que sea una herramienta ilegal.

A la *Dark Web* puede accederse directamente a través de The Hidden Wiki, DuckDuckGo o Tor Browsrer Bundle. No obstante, no es recomendable hacerlo, dadas las consecuencias que puede acarrear. El consejo que debe darse a todo usuario, incluso a quienes pretendan estudiar la ciberdelincuencia, es limitarse a navegar por entornos de red seguros y conocidos.

Dentro de la *Dark Web* encontramos las *Dark Nets*, redes a las cuales solo puede accederse a través de este tipo de servidores y que llevan como dominio «.onion» y no el habitual «.com», lo cual impide acceder a su contenido a toda aquella persona que no tenga en su dispositivo el navegador TOR.

Como muestra puede verse la siguiente captura de pantalla.

Figura 2. Captura de pantalla del escritorio de Hidden Wiki con dominios «.onion»



El uso de la *Dark Web* por parte de las organizaciones terroristas va en aumento debido a las condiciones de seguridad y el anonimato que les garantizan estas herramientas, así como a los elevados recursos que pueden encontrar en su interior que les son útiles para potenciar sus actividades.

1.4. La criptomoneda

Otro aspecto relacionado con el contenido del apartado anterior son las criptomonedas.

> Por definición, las criptomonedas son monedas que no reciben ningún tipo de supervisión por parte de ningún organismo o banco central (es decir, descentralizadas) que se intercambian a través de redes P2P y que están cifradas.

Estas características permiten que las transacciones puedan realizarse sin intermediarios, y que, en consecuencia, sean muy difíciles de rastrear, incluida la información del importe, la identidad del pagador y del beneficiario y el objeto.

Son ejemplos los *bitcoins* o el *dash*. Este último es más complejo técnicamente hablando y, por lo tanto, constituye un instrumento más difícil de trazar por parte de los cuerpos y fuerzas de seguridad.

Todo ello las ha convertido en un medio de pago seguro y atractivo para las organizaciones terroristas, al poder sortear los peligros que presenta el pago en metálico. A este medio se le añaden las facilidades que ofrecen las tarjetas de crédito y la aparición de plataformas como PayPal, aunque estas suponen un riesgo mayor si se compara con la criptomoneda.

2. Ciberseguridad y normativa sobre (ciber)terrorismo

2.1. Prevención y ciberseguridad

El ciberterrorismo cada vez genera más preocupación, pero la complejidad del fenómeno, los diversos actores implicados y los intereses por parte de Estados dificultan la consecución de una normativa común a nivel internacional que sea eficaz para hacer frente al ciberterrorismo y que a la vez sea respetuosa con los derechos y libertades de los ciudadanos. Dadas estas circunstancias, la defensa más efectiva es la ciberseguridad, cuyo objetivo es minimizar el riesgo aplicando una serie de medidas de prevención.

A continuación vamos a describir las medidas en materia de ciberseguridad elaboradas por parte de organismos e instituciones internacionales con el objetivo de hacer frente a las ciberamenazas y ataques por parte de organizaciones terroristas. En el tercer apartado del módulo se va a hacer una breve descripción de los organismos (con el enlace a sus correspondientes páginas) más importantes que trabajan para cumplir con el mandato de las normas sobre ciberseguridad.

2.2. Normativa internacional

Al no existir un documento vinculante de carácter universal, nos limitaremos a citar la resolución más importante de la ONU y a recomendar la lectura del punto 2 («El contexto internacional») del documento ***El uso de internet con fines terroristas de la UNODC***.

El documento más importante en materia de terrorismo es el contenido de la **Estrategia Global contra el terrorismo** (A/RE/60/288) que aprobó en 2006 la Asamblea General, y cuyo contenido alberga todo un conjunto de iniciativas y programas que tienen como objetivos:

Enlace recomendado

Para conocer más en profundidad su contenido puede consultarse el siguiente enlace: Estrategia global de las Naciones Unidas contra el terrorismo, https://undocs.org/es/A/RES/60/288.

1) Hacer frente a las condiciones que propician la propagación del terrorismo.

2) Prevenir y combatir el terrorismo.

3) Desarrollar la capacidad de los Estados miembros para prevenir y combatir el terrorismo y fortalecer el papel del sistema de Naciones Unidas al respecto.

4) Garantizar el respeto universal de los derechos humanos y del estado de derecho como pilar fundamental de la lucha contra el terrorismo.

2.3. Normativa europea

Dada la concienciación que se ha desarrollado en Europa sobre la importancia de luchar contra la ciberdelincuencia y garantizar un ciberespacio seguro, vamos a describir las normas más importantes en materia de ciberseguridad. Se indican, en primer lugar, las normas producidas en el seno del Consejo de Europa y, en segundo lugar, la normativa de la Unión Europea.

1) Convenio sobre el delito cibernético. En 2001 el Consejo de Europa elaboró este documento que, aunque con contenidos mínimos, es actualmente el único instrumento que trata sobre la actividad delictiva en internet. Su contenido debe ser interpretado conjuntamente con otras herramientas jurídicas que buscan el mismo fin. Solo así se podrá elaborar una base jurídica fundamentada en la cooperación que busque detener el uso de internet con fines terroristas.

Enlace recomendado

Para conocer más en profundidad su contenido puede consultarse el siguiente enlace: Convenio sobre el delito cibernético, https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221.

El objetivo principal que quiere conseguir el Convenio es armonizar las distintas legislaciones nacionales existentes sobre delitos cibernéticos para mejorar los mecanismos de detección, investigación y persecución, lo que incluye la obligación de los Estados de elaborar que persigan este fin. El convenio entiende por «delito cibernético» los delitos relacionados con el acceso no autorizado a sistemas, programas o datos informáticos, y la manipulación ilícita de estos; el fraude y la falsificación informáticos, y la tentativa de cometer tales actos o complicidad en su comisión.

2) Decisión marco 2002/475/JAI, de 13 de junio de 2002, sobre la lucha contra el terrorismo, que armoniza la definición de los delitos de terrorismo en todos los Estados miembros de la Unión Europea. En respuesta a la creciente amenaza terrorista, en 2002, el Consejo de la Unión Europea elaboró este documento, a través del cual introdujo una definición específica y común del concepto de delito de terrorismo, entendiéndolo como «[...] delitos graves que se convierten en delitos de terrorismo por razón de la intencionalidad del delincuente. El concepto de delito de terrorismo es, por tanto, una combinación de dos elementos: un elemento objetivo, ya que se refiere a una relación de conductas delictivas graves, tal como se definen con arreglo a la legislación nacional, y un elemento subjetivo, ya que estos actos se considerarán delitos de terrorismo cuando se cometan con una intención determinada [...]» –artículo 3–; esta decisión estableció un conjunto de normas con el objetivo de garantizar que los delitos terroristas fueran perseguidos de manera eficaz y estableció medidas concretas dirigidas a víctimas de delitos de terrorismo. No obstante, cabe decir que esta decisión marco se ha sustituido por la Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo, de 15 de marzo de 2017, relativa a la lucha contra el terrorismo, la cual veremos en este mismo apartado.

3) Decisión Marco 2005/222/JAI, relativa a los ataques contra los sistemas de información. La Decisión de 2005 se había elaborado como respuesta a la amenaza de la delincuencia organizada y la inquietud ante la posibilidad de ataques terroristas contra los sistemas de información que forman parte de infraestructuras vitales de los Estados miembros de la Unión, dejando a cada Estado que legisle al respecto. Aunque de la misma manera que la anterior decisión marco, esta fue sustituida a través de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información.

4) Decisión Marco de 24 de octubre de 2008, relativa a la lucha contra la delincuencia organizada (2008/841/JHA). Tres años después de la anterior, la Decisión Marco 2008/841 surge como sustitución a la Acción Común 98/733/JAI, de 21 de diciembre de 1998, relativa a la tipificación penal de la participación en una organización delictiva en los Estados miembros de la Unión Europea. Tiene por objeto dar respuesta al compromiso que se estableció en el ámbito de la lucha contra el terrorismo, que, dada la naturaleza del fenómeno, requiere reforzar los programas de lucha contra la delincuencia organizada.

Enlace recomendado

Para conocer más en profundidad su contenido puede consultarse el siguiente enlace: Decisión Marco de 24 de octubre de 2008, http://data.europa.eu/eli/dec_framw/ 2008/841/oj.

El **artículo** más importante es el número **2**, al plasmar la voluntad del documento. Concretamente manifiesta que:

> «Todos los Estados miembros adoptarán las medidas necesarias para tipificar como delito a uno o ambos de los siguientes tipos de conducta relacionados con una organización delictiva: (a) la conducta de toda persona que, de manera intencionada y a sabiendas de la finalidad y actividad general de la organización delictiva o de su intención de cometer los delitos en cuestión, participe activamente en las actividades ilícitas de la organización, incluida la facilitación de información o de medios materiales, reclutando a nuevos participantes, así como en toda forma de financiación de sus actividades a sabiendas de que su participación contribuirá al logro de la finalidad delictiva de esta organización; (b) la conducta de toda persona que consista en un acuerdo con una o más personas para proceder a una actividad que, de ser llevada a cabo, suponga la comisión del delito [...]. Por lo tanto, lo que nos viene a decir es que todos los Estados miembros adopten las medidas necesarias para tipificar como delito las conductas propias de organizaciones delictivas».

5) Decisión Marco de 28 de noviembre (2008/919/JAI), relativa a la lucha contra el terrorismo. Nace después de la aparición de células terroristas no estructuradas, no jerárquicas, semiautónomas y ligadas entre ellas en red que recurrían a las nuevas tecnologías para comunicarse, captar nuevos miembros y movilizarse. No obstante, debéis saber que en 2017 esta fue sustituida por la Directiva 2017/541, que veremos más adelante.

Del mismo modo que hemos visto en la anterior decisión marco, este nuevo documento expone en su **artículo 3** que los Estados miembros deben adoptar todas aquellas medidas que estimen necesarias para garantizar la seguridad de sus ciudadanos, lo que implica tipificar como delito de terrorismo todas aquellas conductas que:

- atenten contra la vida o la integridad física de una persona;
- el secuestro o toma de rehenes;

- el apoderamiento ilícito de aeronaves y de buques o de otros medios de transporte colectivo o de mercancías;
- la fabricación, la tenencia, la adquisición, el transporte, el suministro o la utilización de explosivos o armas de fuego, armas químicas, biológicas, radiológicas o nucleares inclusive, así como la investigación y el desarrollo de armas químicas, biológicas, radiológicas o nucleares; y/o
- la liberación de sustancias peligrosas, o la provocación de incendios, inundaciones o explosiones cuyo efecto sea poner en peligro vidas humanas.

Si bien todas estas conductas son más susceptibles de ser realizadas en el mundo real, en la modalidad *online* cobra especial importancia el contenido de los apartados d) y h) del mismo artículo según los cuales también debe considerarse delito de terrorismo:

- (apartado d) las destrucciones masivas de instalaciones estatales o públicas, sistemas de transporte, infraestructuras, sistemas informáticos incluidos, plataformas fijas emplazadas en la plataforma continental, lugares públicos o propiedades privadas, que puedan poner en peligro vidas humanas o producir un gran perjuicio económico; y
- (apartado h) la perturbación o interrupción del suministro de agua, electricidad u otro recurso natural básico cuyo efecto sea poner en peligro vidas humanas. Acciones que de acuerdo con el módulo 1, son susceptibles de ser definidas de ciberterrorismo si son realizadas a través de medios informáticos.

Por otro lado, destacamos el contenido del **artículo 5** («Provocación pública a la comisión de un delito de terrorismo»), ya que defiende que las medidas necesarias para garantizar que se tipifique como delito también deben incorporar «[...] el hecho de difundir o hacer públicos por cualquier otro medio, ya sea en línea o no [...]»; el **artículo 21** («Medidas contra los contenidos en línea que constituyan provocación pública»), donde se expone que «Los Estados miembros adoptarán las medidas necesarias para garantizar la rápida eliminación de los contenidos en línea albergados en su territorio [...]» o « [...] los Estados miembros podrán adoptar medidas para bloquear el acceso a dicho contenido por parte de los usuarios de internet dentro de su territorio».

Dada la importancia de este documento, es necesario saber cómo la Unión Europea define «infraestructura crítica». Según el Programa de Infraestructuras Críticas, estas son:

«aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los Gobiernos de los Estados miembros».

A su vez, estas las podemos clasificar atendiendo a dos criterios: según propiedad (públicas o privadas); y según criterios sectoriales (centrales y redes de energía; tecnologías de las comunicaciones y la información; finanzas; salud; alimentación; agua; transporte; producción, almacenamiento y transporte de mercancías peligrosas). No obstante, la UE es consciente de que en plena globalización la delimitación territorial es confusa y difícil, siendo mejor hablar de interdependencia, un aspecto que las hace ser vulnerables a posibles ciberataques terroristas. Por este motivo, si se quiere proteger este tipo de infraestructuras, se requiere un trabajo cooperativo y sincronizado, razón por la que se creó la Red de Alertas en Infraestructuras Críticas (CIWIN o Critical Infraestructures Warning Information Network).

6) Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo. Esta directiva tiene como objetivo el de aproximar las normas de derecho penal de los Estados miembros en materia de ataques contra los sistemas de información, mediante el establecimiento de normas mínimas relativas a la definición de las infracciones penales y las sanciones aplicables, y mejorar, así, la cooperación entre las autoridades competentes, incluida la policía y los demás servicios especializados encargados de la aplicación de la ley en los Estados miembros, así como los organismos especializados de la Unión, como Eurojust, Europol y su Centro Europeo contra la Ciberdelincuencia y la Agencia Europea de Seguridad de las Redes y de la Información (ENISA).

Los sistemas de información son un elemento esencial para la interacción política, social y económica en la Unión, y el aumento de estos lleva a la Directiva a poner énfasis en su definición para luego considerar aspectos como son las infraestructuras críticas, los ataques de gran escala y los ciberataques. Es importante, por tanto, en esta materia disponer de definiciones comunes a fin de garantizar la aplicación coherente de la Directiva en los Estados miembros.

Las diferencias y divergencias significativas que existen entre las legislaciones y los procesos penales de los Estados miembros en este ámbito pueden dificultar la lucha contra la delincuencia organizada y el terrorismo y complicar la cooperación policial y judicial efectiva en este ámbito. La naturaleza transna-

Lecturas recomendadas

Para un mayor análisis véase:

J. L. González Cussac (2006). «El Derecho Penal frente al Terrorismo». En: J. L. Gómez Colomer; J. L. González Cussac. *Terrorismo y proceso penal acusatorio*. Valencia: Tirant lo Blanch.

E. Agudo Fernández; M. Jaén; A. Perrini (2016). «Los delitos de terrorismo en el Código Penal». En: *Terrorismo en el siglo XXI: La respuesta penal en el escenario mundial*. Madrid: Dykinson.

R. García Albero (2016). «Comentarios a los artículos 571 ss.». En: G. Quintero (dir.). Comentarios a la parte especial del Derecho Penal (7.ª ed.) (págs. 1884-1945). Cizur Menor: Aranzadi.

Enlace recomendado

Para conocer más en profundidad su contenido puede consultarse la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo. Enlace:

http://data.europa.eu/eli/dir/2013/40/oj.

cional y transfronteriza de los modernos sistemas de información significa que los ataques suelen revestir un carácter transfronterizo, lo que plantea la necesidad urgente de proseguir la aproximación del derecho penal en este ámbito.

Por tanto, el objetivo principal de la Directiva es el de garantizar que los ataques contra los sistemas de información sean castigados en todos los Estados miembros con penas efectivas, proporcionadas y disuasorias, y mejorar y fomentar la cooperación judicial entre las autoridades judiciales y otras autoridades competentes, dado que no pueden ser alcanzados de manera suficiente por los Estados miembros, y que, por consiguiente, debido a sus dimensiones o efectos, pueden lograrse mejor a escala de la Unión.

7) Directiva (UE) 2016/1148 Del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Las redes y sistemas de información desempeñan un papel crucial en la sociedad. Su fiabilidad y seguridad son esenciales para las actividades económicas y sociales, y en particular para el funcionamiento del mercado interior de la UE. Asimismo, la magnitud, la frecuencia y los efectos de los incidentes de seguridad se están incrementando y representan una grave amenaza para el funcionamiento de las redes y sistemas de información. Esos sistemas pueden convertirse, además, en objetivo de acciones nocivas deliberadas destinadas a perjudicar o interrumpir su funcionamiento. Este tipo de incidentes puede interrumpir las actividades económicas, generar considerables pérdidas financieras, menoscabar la confianza del usuario y causar grandes daños a la economía de la Unión.

Por ello, la Directiva establece medidas con el objeto de lograr un elevado nivel común de seguridad de las redes y sistemas de información dentro de la Unión a fin de mejorar el funcionamiento del mercado interior. A tal fin, la Directiva:

- establece obligaciones para todos los Estados miembros de adoptar una estrategia nacional de seguridad de las redes y sistemas de información;
- crea un Grupo de cooperación para apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros y desarrollar la confianza y seguridad entre ellos;
- crea una red de equipos de respuesta a incidentes de seguridad informática (en lo sucesivo, «red de CSIRT», por sus siglas en inglés Computer Security Incident Response Teams) con el fin de contribuir al desarrollo de la confianza y seguridad entre los Estados miembros y promover una cooperación operativa rápida y eficaz;
- establece requisitos en materia de seguridad y notificación para los operadores de servicios esenciales y para los proveedores de servicios digitales;
- establece obligaciones para que los Estados miembros designen autoridades nacionales competentes, puntos de contacto únicos y CSIRT con fun-

ciones relacionadas con la seguridad de las redes y sistemas de información.

8) Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo, de 15 de marzo de 2017, relativa a la lucha contra el terrorismo y por la que se sustituye la Decisión marco 2002/475/JAI del Consejo y se modifica la Decisión 2005/671/JAI del Consejo. La Directiva establece normas mínimas relativas a la definición de las infracciones penales y las sanciones en el ámbito de los delitos de terrorismo, los delitos relacionados con un grupo terrorista y los delitos relacionados con actividades terroristas, así como medidas de protección, apoyo y asistencia a las víctimas del terrorismo.

Una de las cuestiones relevantes de la Directiva es la referida a las medidas contra los contenidos en línea que constituyan provocación pública (art. 21). Por ello establece lo siguiente:

> «Los Estados miembros adoptarán las medidas necesarias para garantizar la rápida eliminación de los contenidos en línea albergados en su territorio constitutivos de provocación pública a la comisión de un delito de terrorismo [...]».

Y en el mismo artículo se remite al 5, donde se precisa que:

> «Los Estados miembros adoptarán las medidas necesarias para garantizar que se tipifique como delito, cuando se cometa intencionadamente, el hecho de difundir o hacer públicos por cualquier otro medio, ya sea en línea o no, mensajes destinados a incitar a la comisión de uno de los delitos enumerados en el artículo 3 de la Directiva».

2.4. Legislación española

Dadas las normas que se derivan de los documentos que acabamos de estudiar, cada Estado miembro debe realizar acciones dirigidas a la ciberseguridad y ciberdefensa. Esto incluye la elaboración de leyes, protocolos, programas y actividades que incluyan la sensibilización y formación entre profesionales.

Antes de entrar a profundizar en la modificación del Código Penal en materia de terrorismo, consideramos importante destacar los siguientes documentos:

1) Real Decreto Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. El Decreto pretende reforzar las acciones de ciberseguridad al concebir que las herramientas actuales no bastan para garantizar un óptimo nivel de seguridad en redes y sistemas de información. Unas acciones que son sumamente necesarias si tenemos en cuenta que estas infraestructuras tienen un papel crucial en la sociedad y en la actividad económica y política que en ellas se realizan.

2) El Real Decreto Ley 12/2018 transpuso el contenido de la Directiva 2016/1148. En este documento se define el «servicio digital» como «el servicio de la sociedad de la información prestado habitualmente a título oneroso, a distancia, por vía electrónica y a petición del interesado». Sin embargo, la ley

solo afecta a aquellas empresas con más de 50 empleados y con un volumen de negocio anual superior a los 10.000.000 de euros, al considerar que son las que mayoritariamente proveen de servicios digitales. Por consiguiente, este tipo de empresas o instituciones deben garantizar:

- la seguridad de los sistemas e instalaciones;
- la correcta gestión de incidentes, así como la continuidad de las actividades. De ello se encargan tres instituciones: el Centro Criptológico Nacional-Computer Emergency Response Team –CCN-CERT–, el Instituto Nacional de Ciberseguridad-Computer Emergency Response Team (INCIBE-CERT) y el Ministerio de Defensa;
- la supervisión, auditorías y pruebas necesarias; y
- el cumplimiento de las normas internacionales.

Declaración ministerial de administración electrónica de Tallin

En 2017 España suscribió este documento, cumpliendo con los objetivos marcados en el Plan de Acción sobre Administración Electrónica de la Unión Europea que debe desarrollarse en su integridad en 2022. Esta declaración tiene como objetivo garantizar que toda empresa y ciudadano europeo pueda interactuar digitalmente con la Administración pública, basándose en los principios de fiabilidad y seguridad; de apertura y transparencia e interoperabilidad por defecto.

2.4.1. Delitos de terrorismo

El Código Penal define los delitos de terrorismo en el art. 573. Según su redacción, se considerará delito de terrorismo la comisión de cualquier delito grave contra la vida o la integridad física, la libertad, la integridad moral, la libertad e indemnidad sexuales, el patrimonio, los recursos naturales o el medio ambiente, la salud pública, de riesgo catastrófico, incendio, de falsedad documental, contra la Corona, de atentado y tenencia, tráfico y depósito de armas, municiones o explosivos, previstos en el presente Código, y el apoderamiento de aeronaves, buques u otros medios de transporte colectivo o de mercancías, cuando se llevaran a cabo con cualquiera de las siguientes finalidades:

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

2) Alterar gravemente la paz pública.

3) Desestabilizar gravemente el funcionamiento de una organización internacional.

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

No obstante, cabe decir que la regulación de los delitos de terrorismo ha sufrido diversas modificaciones desde la aprobación del Código Penal de 1995, de las que merecen ser destacadas las introducidas por la **Ley Orgánica 2/2015,**

de reforma del CP en materia de terrorismo, que modifica el capítulo VII del título XXII y comprende los arts. 571 a 580, y la **LO 1/2019, de 20 de febrero**, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, para transponer Directivas de la Unión Europea en los ámbitos financiero y de terrorismo y abordar cuestiones de índole internacional.

Las reformas han afectado, entre otras tipologías, al delito de adoctrinamiento, descrito en el **artículo 575**, cuya modificación se produjo como respuesta a la Decisión Marco 2002/475/JAI del Consejo de la Unión Europea, de 13 de junio de 2002, sobre la lucha contra el terrorismo, modificada por la Decisión Marco 2008/919/JAI, de 28 de noviembre de 2008. De esta manera pasa a ser penalmente castigado aquel o aquellas que:

> «[...] con la finalidad de capacitarse para llevar a cabo cualquiera de los delitos tipificados en este capítulo, reciba adoctrinamiento o adiestramiento militar o de combate –artículo 575.1– [...]. Se entenderá que comete este delito quien, con tal finalidad, acceda de manera habitual a uno o varios servicios de comunicación accesibles al público en línea o contenidos accesibles a través de internet [...]. Asimismo se entenderá que comete este delito quien, con la misma finalidad, adquiera o tenga en su poder documentos que estén dirigidos o, por su contenido, resulten idóneos para incitar a la incorporación a una organización o grupo terrorista o a colaborar con cualquiera de ellos o en sus fines –artículo 575.2– [...]. La misma pena se impondrá a quien, para ese mismo fin, o para colaborar con una organización o grupo terrorista, o para cometer cualquiera de los delitos comprendidos en este capítulo, se traslade o establezca en un territorio extranjero controlado por un grupo u organización terrorista –artículo 575.3–».

Este último apartado ha sido modificado en 2019 a través de la LO 1/2019, de 20 de febrero, para transponer la Directiva UE de 15 de marzo de 2017 relativa a la lucha contra el terrorismo. Con la nueva redacción se elimina la exigencia de que el desplazamiento se produzca hacia una zona controlada por la organización terrorista:

> «La misma pena se impondrá a quien, para ese mismo fin, o para colaborar con una organización o grupo terrorista, o para cometer cualquiera de los delitos comprendidos en este Capítulo, se traslade o establezca en un territorio extranjero».

También se introduce, mediante la LO 1/2019, un nuevo artículo 580 bis, en virtud del cual la responsabilidad penal de las personas jurídicas se extiende a todos los delitos de terrorismo tipificados en el capítulo. La Directiva de 2017 daba pie a ello, aunque al ser tan amplio el catálogo de delitos de terrorismo previsto en el CP español el número de supuestos por los que las empresas podrían incurrir en responsabilidad penal corporativa es tan elevado que podemos afirmar que, también en este caso, el legislador ha incurrido en desmesura (García Albero, 2019).

Además de la definición, otras de las novedades que introdujo la LO 2/2015 fue la figura del adoctrinamiento (art. 575.1) y autoadoctrinamiento (art. 575.2), definiéndolo como:

«capacitarse para cometer alguno de los delitos tipificados (en materia de terrorismo)» [...] «se entenderá que comete este delito quien, con tal finalidad, acceda de manera habitual a uno o varios servicios de comunicación accesibles al público en línea o contenidos accesibles a través de internet o de un servicio de comunicaciones electrónicas cuyos contenidos estén dirigidos o resulten idóneos para incitar a la incorporación a una organización o grupo terrorista, o a colaborar con cualquiera de ellos o en sus fines. [...] Asimismo, se entenderá que comete este delito quien, con la misma finalidad, adquiera o tenga en su poder documentos que estén dirigidos o, por su contenido, resulten idóneos para incitar a la incorporación a una organización o grupo terrorista o a colaborar con cualquiera de ellos o en sus fines».

2.4.2. Delitos informáticos con fines terroristas

Por último, debe tenerse en cuenta lo previsto en el art. 573.2 del CP, según el cual se consideran delitos de terrorismo los previstos en los artículos 197 bis y 197 ter (acceso a sistemas de información e intercepción de datos informáticos) y 264 y 264bis (daños informáticos), cuando se realicen con alguna de las finalidades de carácter terrorista a las que alude el Código, concretamente las mencionadas en el punto anterior (art. 573.1). Ello tiene como consecuencia la aplicación de la pena superior en grado a la prevista legalmente para los respectivos delitos (en virtud del art. 573 bis-3), lo cual plantea complejas cuestiones de *bis in idem*, dada la cualificación que a su vez prevé el Código en los indicados delitos comunes.

Enlace recomendado

Para conocer el contenido de las normas penales es imprescindible consultar directamente el CP. Concretamente, la Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo. https://www.boe.es/buscar/doc.php?id=BOE-A-2015-3440.

Por lo tanto, podemos concluir que en España el (ciber)terrorismo se está combatiendo, legalmente, mediante el adelantamiento de la barrera punitiva, ampliando de manera desmesurada los casos en los que puede aplicarse el concepto de «terrorismo». Un adelantamiento de la intervención penal que, como han criticado diversos autores, se sitúa hasta la mera ideación subjetiva (Guirao, 2009).

3. Estrategias desarrolladas contra el ciberterrorismo

Las características de la red dificultan el rastreo de actividades ciberterroristas. Por este motivo no se disponen de herramientas eficaces para su detección y prevención. A continuación describiremos aquellas estrategias que se están utilizando con estos fines, así como las instituciones que están poniendo sus esfuerzos en contener dicha actividad.

3.1. Estrategias para la lucha contra el terrorismo

La lucha antiterrorista constituye una prioridad para diversos organismos, instituciones y Estados. A raíz de ello se han ido adoptando distintas iniciativas con el objetivo de intentar prevenir, proteger, perseguir y responder a futuros atentados que estas organizaciones vayan a poder cometer en el mundo *offline* u *online*, incluidas las de carácter económico.

Enlace recomendado

A nivel europeo puede consultarse el enlace al documento *IOCTA* (*Internet, Organised, Crime, Threat and Assessment*) de 2018. En él puede encontrarse un resumen de la Europol sobre las tendencias reportadas en cibercrimen, incluido el ciberterrorismo.

Enlace: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018.

Algunas de las estrategias más utilizadas por parte de la Unión Europea desde 2005 son:

- Reforzar la legislación en materia de terrorismo.
- Intensificar los controles en las fronteras exteriores.
- Intensificar el control de la compra y venta de armas y material químico susceptible de poder ser utilizado para la fabricación de explosivos.
- La creación de organismos específicos destinados a controlar y frenar la proliferación en el ciberespacio de sitios que alienten el terrorismo como, por ejemplo, a través de propaganda o publicaciones en línea.

1) Reglamento del uso de los datos del registro de nombres de los pasajeros (también conocida por sus siglas PNR). Esta estrategia fue adoptada por la Unión Europea dentro del marco de la lucha antiterrorista a través de la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros y se dirige a: compañías aéreas, titulares de las aeronaves en el caso de vuelos privados y entidades de gestión de reserva de vuelos. Estos datos deben servir para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave.

El objetivo de la Directiva es elaborar un registro único integrado por datos personales de pasajeros con el fin de que puedan ser consultados por cualquier Estado siempre que su finalidad sea la prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos graves y se haya hecho la oportuna ponderación entre riesgos y beneficios. Por este motivo, se insta a todos los Estados miembros a crear una unidad de información sobre los pasajeros con una persona al frente responsable de la protección de sus datos: la Unidad

de Información sobre Pasajeros (UIP). Esta se encarga de recoger, tratar y analizar los datos que integraran la PNR, así como de gestionar las comunicaciones e intercambios con las autoridades competentes nacionales, UIP de otros estados miembros, y con la Europol. Una vez se recopilan los datos, la UIP tiene entre 24 y 48 horas antes de la salida del vuelo para enviarlos al órgano central. En el caso concreto de España, esta pertenece al Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO).

La creación del PNR, como hemos dicho, limita el tratamiento de los datos a las finalidades legítimas de acuerdo con el derecho a la protección de los datos personales. De acuerdo con dicha directiva:

- No se pueden recoger o utilizar datos sensibles de los pasajeros.
- Una vez recogidos los datos, pasados seis meses estos deben ser despersonalizados. Es decir, el contenido de la información no puede ser susceptible de ser relacionado con la persona.
- Los datos solo pueden conservarse durante cinco años; después deben ser eliminados.
- Los Estados miembros deben asegurarse de que los pasajeros reciben una información clara sobre la recogida de datos PNR y sus derechos.
- La transferencia de datos PNR a terceros países solo podrá producirse en circunstancias muy particulares y deberá estudiarse caso por caso.

Enlace recomendado

Puede consultarse la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros: https://www.boe.es/buscar/doc.php?id=DOUE-L-2017-80815.

De esta manera, adoptando estos criterios, se protege el derecho fundamental a la protección de los datos personales.

2) Estrategia nacional de Ciberseguridad. En abril de 2019, España publicó la Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional. A través de esta se publicaron las estrategias nacionales de seguridad aeroespacial, de protección civil y de ciberseguridad. Debemos remarcar que lejos de la falta de consenso en anteriores iniciativas (incluso en la definición de «ciberterrorismo»), estas estrategias han sido elaboradas con el asesoramiento de expertos de los ámbitos público y empresarial en cada una de las áreas, y con el consenso de las comunidades autónomas.

Enlaces recomendados

Puede consultarse la Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional:

https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-6347.

Acceso directo a la descarga en abierto del documento *Estrategia Nacional Contra el Terrorismo 2019*:

https://www.dsn.gob.es/es/documento/ estrategia-nacional-contra-terrorismo-2019.

En el ámbito del ciberterrorismo, el capítulo 2 expone la preocupación hacia este ámbito, así como la voluntad de alcanzar un ciberespacio seguro que pueda hacer frente al ciberterrorismo. De esta manera, se justifica la necesidad de reforzar el trabajo en la prevención y detección de este tipo de ciberconductas. Concretamente manifiesta que:

> «Los grupos terroristas tratan de aprovechar las vulnerabilidades del ciberespacio para realizar ciberataques o para actividades de radicalización de individuos y colectivos, financiación, divulgación de técnicas y herramientas para la comisión de atentados, y de reclutamiento, adiestramiento o propaganda. Íntimamente relacionado con ello, se halla la amenaza contra las infraestructuras críticas, con la posibilidad cierta de causar un colapso a través de las redes mediante una caída en cadena de los servicios esenciales».

Por todo ello, la Estrategia se basa en cuatro principios:

- **Unidad de acción:** establece que la respuesta a un ciberataque (como puede ser aquel cometido por una organización terrorista) debe implicar a los distintos agentes del Estado. A su vez, sus acciones han de ser coherentes y estar coordinadas.
- **Anticipación:** defiende que las actuaciones en materia de ciberseguridad deben priorizar la acción preventiva por encima de la reactiva. Para ello se requiere un sistema de información compartida que pueda ser consultado por cualquier agente responsable en el ámbito de la ciberseguridad que permita tomar decisiones en el menor tiempo posible. Este es un aspecto clave si queremos reducir las ciberamenazas.
- **Eficiencia:** la ciberseguridad requiere un equipo multidisciplinar de profesionales y que cuente con programas y softwares con un elevado nivel tecnológico. Una necesidad que surge ante la complejidad que conlleva el terrorista. Recordemos la capacidad adaptativa que tiene el fenómeno, incluso en la red.
- **Resiliencia:** si bien es un término que utilizamos para referirnos a la capacidad que tienen algunas personas para sobreponerse a adversidades traumáticas vividas, en el ámbito de la cibercriminalidad también se utiliza para referirse a la capacidad que deben tener las estructuras (informáticas) críticas de rehacerse de los efectos que pueden producir en ellas las ciberamenazas y ciberataques. De este modo, el Estado está obligado a dotarlas de todos aquellos elementos que considere necesarios para garantizar su protección frente a este tipo de ciberataques.

3.2. Instituciones que combaten el ciberterrorismo

1) EUROJUST: a nivel europeo, en 2002 el Consejo de Europa adoptó la Decisión 2002/187/JHA, por la que se crea EUROJUST, la Unidad de Cooperación Judicial de la Unión Europea, con sede en La Haya. Su nacimiento surgió con un doble objetivo. Por un lado, reforzar la cooperación y la lucha contra las formas graves de delincuencia, incluida la informática; por otro, mejorar la cooperación judicial entre los 28 Estados miembros. Por este motivo, cada uno de los Estados miembros nombra un representante de alto nivel (fiscales, jueces o funcionarios de policía con competencias equivalentes) para trabajar en EUROJUST.

En referencia al terrorismo, en noviembre de 2018, tras la Cumbre Europea contra el Terrorismo celebrada en París, EUROJUST acordó una serie de medidas, entre las que destacan:

- Crear un registro judicial en materia de terrorismo que permita a los Estados miembros poder consultar para identificar elementos comunes entre diferentes casos abiertos en materia terrorista.
- Desarrollar herramientas que permitan la eliminación de contenidos terroristas de internet con el objetivo de prevenir la difusión de la ideología yihadista.
- Establecer el compromiso de mejorar la cooperación entre los Estados con el fin de ofrecer un mejor servicio de apoyo a todas las víctimas del terrorismo.

Enlace recomendado

Pueden consultarse los proyectos en los que trabaja EUROJUST en:

http://eurojust.europa.eu/Pages/ languages/es.aspx.

2) ENISA (Agencia de la Unión Europea para la Ciberseguridad). El Consejo Europeo también creó en 2004 la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) con sede en Atenas (Grecia). Es un organismo encargado de trabajar en favor de la seguridad cibernética. Para ello brinda su apoyo a los Estados miembros y a las partes interesadas de la Unión Europea (incluidos actores privados), para dar así respuesta a ciberataques sufridos, incluidos aquellos que pueden producirse entre los propios Estados.

Entre sus funciones destacan:

- Analizar riesgos actuales y emergentes que puedan poner en peligro la resistencia y disponibilidad de las redes de comunicación electrónicas.
- Mejorar la cooperación entre los agentes que operan en el campo de seguridad de las redes y de la información.
- Asistir a la Comisión y a los Estados miembros en su diálogo con el sector industrial para hacer frente a los problemas relacionados con la seguridad en los equipos y programas informáticos.
- Promover actividades de evaluación de riesgos, soluciones interoperables de gestión del riesgo y estudios sobre soluciones de gestión de la prevención dentro de las organizaciones de los sectores público y privado.
- Elaborar y ofrecer recomendaciones sobre ciberseguridad y asesoramiento a los Estados miembros y a las partes interesadas de la Unión Europea.

Enlaces recomendados

Para conocer todos los proyectos en los que trabaja la EUROPOL, podéis acceder al siguiente enlace:

https://www.europol.europa.eu/.

Los informes y otra información sobre terrorismo pueden encontrarse en el siguiente enlace:

https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/terrorism?ct[article]=article&ct[event]=event&ct[guide]=guide&ct[panel]=panel&ct[multimedia]=multimedia&ct[news]=news&ct[operation]=operation&ct[page]=page&ct[document]= document.

Además, desde 2019, coincidiendo con la entrada en vigor del Reglamento 2019/881, ENISA también prepara los esquemas de certificación europeos de ciberseguridad a través de los cuales se garantizará que los productos, servicios y procesos que se comercializan en territorio de la UE cumplen con unos estándares, pero dicha certificación no será obligatoria hasta 2023.

3) EUROPOL: es un organismo de la Unión Europea con sede en La Haya (Países Bajos) que centra su actividad investigadora en luchar contra la gran delincuencia, entendida esta como: el terrorismo, el tráfico de drogas y el blanqueo de capitales a nivel internacional; el fraude organizado; la falsificación de euros; la trata de personas; así como los nuevos peligros que están surgiendo tras la implantación de las TIC, lo que conocemos como ciberdelincuencia. Su trabajo consiste en asesorar a países de la UE y aquellos que no son miem-

bros pero sí asociados, brindan su apoyo a operaciones policiales y publican informes sobre la situación y tendencia de cada una de las tipologías anteriormente citadas.

En el caso del terrorismo, debe tenerse en cuenta la información que contienen los informes *Europol's EU Terrorism Situation and Trend Report* (TE-SAT), que publica anualmente en su página web y en los cuales podréis observar la evolución que ha tenido el fenómeno desde 2007, año en que se publicó el primero.

Resumen

En este módulo hemos podido conocer que el ciberespacio es más complejo de lo que a priori puede parecer. Hemos visto que la información que subyace en cada uno de sus niveles, mediante la metáfora del iceberg, es inmensa. También se ha tomado conciencia de que solo conocemos una ínfima parte de su totalidad y que las actividades de los ciberterroristas se llevan a cabo en la *Dark Net* mediante el uso de navegadores como TOR.

Por otro lado, hemos estudiado las implicaciones que tiene el uso de internet por parte de organizaciones terroristas en el sistema jurídico actual, tanto a nivel internacional y europeo como en el caso español; así como el abordaje que se está haciendo desde instituciones y organizaciones como EUROJUST, ENISA y EUROPOL. De manera más concreta, se han examinado algunas iniciativas que se están tomando, como el PNR. Sin embargo, de cara al futuro, los retos que se nos presentan son diversos y complejos, ya que en los próximos años la preocupación sobre ciberseguridad se centrará en la implementación de la red 5G y los efectos que pueda conllevar su utilización por parte de grupos cibercriminales. Por ello, la Comisión Europea ya ha empezado a preparar estrategias cuyo objetivo es alcanzar una mayor cooperación entre Estados que garantice el intercambio de información entre los miembros de la Unión.

Ejercicios de autoevaluación

Para que podáis comprobar el grado de consolidación que habéis alcanzado tras el estudio del material, os proponemos contestar diez preguntas tipo test.

1. ¿Qué significan las siglas TOR?

a) Terrorism On Router
b) The Onion Router
c) Terrorism Online Router
d) The Origin Router

2. *Clear net* es...

a) el internet que utilizan las organizaciones terroristas para comprar armas.
b) el internet que representa el 1 % del total de la red.
c) el internet que utiliza IP enmascaradas.
d) el internet al que todos nosotros podemos acceder. Por ejemplo, a través de búsquedas en Google.

3. ¿Qué característica del ciberespacio garantiza TOR?

a) Anonimato.
b) Introyección solipsista.
c) Invisibilidad.
d) Las respuestas a) y b) son correctas.

4. La *Deep Web*...

a) forma parte de la *clear net*.
b) es el segundo nivel de la red y no tiene por qué ser siempre sinónimo de actividad criminal.
c) ocupa la parte más profunda en el ciberespacio.
d) es el segundo nivel de la red en el que se realizan todo tipo de actividades ilegales, siendo la compra y venta de armas la más realizada.

5. Indicad cuál de las siguientes afirmaciones sobre la PRN es incorrecta:

a) No se pueden recoger o utilizar datos sensibles de los pasajeros.
b) Los datos nunca se deben borrar del registro, excepto en aquellas circunstancias que así lo indique Europol.
c) Pasados seis meses los datos deben ser despersonalizados.
d) Cada Estado debe tener una UIP.

6. La Estrategia Nacional de Ciberseguridad se estructura en torno a cinco principios...

a) Unidad de acción, anticipación, eficacia y resiliencia.
b) Unidad de acción, anticipación, solidaridad y resiliencia.
c) Unidad de acción, eficacia, solidaridad y cooperación.
d) Unidad de acción, anticipación, eficiencia y resiliencia.

7. ¿Cuál de las convenciones elaboradas por parte del Consejo de Europa es la única vinculante para la lucha contra el uso de internet con fines terroristas?

a) Decisión Marco de 28 de noviembre, relativa a la lucha contra el terrorismo.
b) Decisión Marco relativa a los ataques contra los sistemas de información.
c) Decisión Marco, de 13 de junio de 2002, sobre la lucha contra el terrorismo, que armoniza la definición de los delitos de terrorismo en todos los Estados miembros de la Unión Europea.
d) Actualmente no existe ninguna cuyo contenido sea vinculante.

8. Indicad cuál de las siguientes afirmaciones sobre EUROPOL es verdadera:

a) Es una institución de Naciones Unidas.

b) Solo atiende a países miembros de la UE.
c) De su actividad investigadora se elaboran informes que no se publican en abierto.
d) EUROPOL investiga sobre: el terrorismo, el tráfico de drogas y el blanqueo de capitales a nivel internacional; el fraude organizado; la falsificación de euros; la trata de personas; y los nuevos peligros que están surgiendo tras la implantación de las TIC, lo que conocemos como ciberdelincuencia.

9. El Reglamento del uso de los datos del registro de nombres de los pasajeros se dirige a...

a) compañías aéreas, titulares de las aeronaves en el caso de vuelos privados; y entidades de gestión de reserva de vuelos.
b) compañías aéreas internacionales y helipuertos.
c) compañías aéreas, titulares de las aeronaves en el caso de vuelos privados; entidades de gestión de reserva de vuelos y titulares de drones.
d) los pasajeros que deben identificarse y rellenar un formulario cada vez que compren un billete de avión o tren.

10. La novedad que introdujo la LO 2/2015 en el Código Penal español ha sido...

a) la eliminación de la exigencia que imponía el art. 575.3 de que el desplazamiento se produzca hacia una zona controlada por la organización terrorista.
b) una definición unánimemente compartida por todos los países de la UE sobre lo que se debe entender por terrorismo.
c) el delito de autoadoctrinamiento recogido en el artículo 575.2.
d) que introduce cuatro conductas ciberterroristas como penalmente punibles.

Solucionario

Ejercicios de autoevaluación

1. b

2. d

3. a

4. b

5. b

6. d

7. c

8. d

9. a

10. c

Bibliografía

Agudo Fernández, E.; Jaen, M.; Perrini, A. (2016). «Los delitos de terrorismo en el Código Penal». En: *Terrorismo en el siglo xxi: La respuesta penal en el escenario mundial*. Madrid: Dykinson.

Akhgar, B.; Brewster, B. (eds.) (2016). *Combating cybercrime and cyberterrorism: challenges, trends and priorities*. Springer.

Bergman, M. K. (2001). «White paper: the deep web: surfacing hidden value». *Journal of electronic publishing* (núm. 1, vol. 7).

Cano, M. A.; Castro, F. J. (2018). «El camino hacia la (ciber)yihad. Un análisis de las fases del proceso de radicalización islamista y su interpretación por parte de los tribunales españoles a partir de los datos suministrados por sentencias judiciales». *Revista electrónica de ciencia penal y criminología* (núm. 16, vol. 20).

Cuerda Arnau, M. L.; Hernández Fernández, A. (2019). *Adoctrinamiento, adiestramiento y actos preparatorios en materia terrorista*. Cizur Menor: Thomson Reuters Aranzadi.

Dinniss, H. A. H. (2018). «The Threat of Cyber Terrorism and What International Law Should (Try To) Do about It». *Georgetown Journal of International Affairs* (vol. 19, págs. 43-50).

García Albero, R.; Quintero, G. (dir.) (2016). *Comentarios a la parte especial del Derecho Penal* (7.ª ed.). Cizur Menor: Aranzadi.

García Albero, R. (2016). «Comentarios a los artículos 571 ss.». En: G. Quintero (dir.). *Comentarios a la parte especial del Derecho Penal* (7.ª ed.) (págs. 1884-1945). Cizur Menor: Aranzadi.

García Albero, R. (2019). «La nueva responsabilidad penal de las personas jurídicas en el delito de malversación y otras reformas –aparentemente– menores». En: G. Quintero y otros. *Las reformas penales de 2019* (págs. 119-133). Cizur Menor: Aranzadi.

González Cussac, J. L. (2006). «El Derecho Penal frente al Terrorismo». En: J. L. Gómez Colomer; J. L. González Cussac. *Terrorismo y proceso penal acusatorio*. Valencia: Tirant lo Blanch.

Guirao, M. C. (2019). «El Delito de autoadoctrinamiento: ¿adelantamiento de la intervención penal a la mera ideación subjetiva? Análisis de sentencias». *Indret*.

Liang, Y.; Chi, Z. (2018). «Analytical Insights on Criminal Law Legislation of Anti-Cyberterrorism». *China Legal Sci.* (núm. 69, vol. 6).

Presidencia de Gobierno (2019). *Estrategia Nacional Contra el Terrorismo 2019*. <https://www.dsn.gob.es/es/documento/estrategia-nacional-contra-terrorismo-2019>.

UNODC (2013). *El uso de internet con fines terroristas*. Naciones Unidas. <https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_Internet_Ebook_SPANISH_for_web.pdf>.