EL USO DE LAS NUEVAS TECNOLOGÍAS POR EL TERRORISMO YIHADISTA

RODRIGO LODEIRO CORRAL

COMANDANTE DE LA GUARDIA CIVIL. SECCIÓN DE OPERACIONES DEL ESTADO MAYOR DE MANDO DE OPERACIONES DE LA GUARDIA CIVIL

RESUMEN

Partiendo de las diferentes publicaciones oficiales que existen sobre esta materia, especialmente el documento “El uso de Internet con fines terroristas” de la Oficina de las Naciones Unidas contra la Droga y el Delito, este artículo tiene como finalidad el análisis de los actuales instrumentos que, principalmente desde el punto de vista judicial, técnico y policial, existen. Y, por otro lado, fruto de las entrevistas mantenidas con expertos de la lucha antiterrorista y la experiencia del autor en esta materia, proponer cuáles serían los instrumentos idóneos y cuál sería el camino a seguir para invertir el imparable aumento en la utilización de las nuevas tecnologías, por parte de las organizaciones terroristas de carácter yihadista, para cometer atentados o acciones terroristas.

Hay circunstancias que convierten a España en objetivo del terrorismo internacional: la vecindad con regiones inestables como el Sahel, la posible y creciente radicalización de los emigrantes tanto de primera como de segunda generación, las reivindicaciones del islamismo radical sobre este país como parte del imaginario del Islam, y su determinante implicación en la lucha contraterrorista.

El uso de las nuevas tecnologías, con la finalidad última de cometer una acción terrorista al uso o en la modalidad de ciberataque, es un problema transnacional que exige una acción coordinada e integrada entre los diferentes estados del sistema interestatal.

Sin embargo, a la ausencia de una gobernanza global de Internet, se suma otra gran dificultad a la hora de establecer una estrategia global contra este fenómeno, que es la necesidad de conocimientos técnicos para la investigación eficaz de estos delitos, así como la homologación de los procedimientos utilizados para obtención de información y garantizar su validez para sostener la imputación en el posterior proceso penal.

Por otro lado, una estrategia eficaz contra el terrorismo a través de las nuevas tecnologías exige una cooperación policial ágil e implicación de todos los actores competentes en el asunto: Estados miembros de las principales Organizaciones Internacionales, servicios policiales, de inteligencia, del ámbito de la ciberdefensa jueces y compañías proveedoras de servicios de tecnologías de la información.

Palabras clave: ciberyihad, nuevas tecnologías, redes sociales, mensajería instantánea, reclutamiento¸ radicalización, incitación al terrorismo, financiación, adiestramiento y planificación.

ABSTRACT

On the basis of the various official publications on this subject, in particular the document “Internet use for terrorist purposes” of the United Nations Office on Drugs and Crime, this article has the purpose of analyzing the currently existing instruments, mainly from the judicial, technical and police point of view. On the other hand, as a result of interviews with experts on the fight against terrorism and the author’s experience in this area, this article proposes what the ideal instruments would be and what the way to continue to reverse the unstoppable increase in the use of new Technologies, would be by terrorist organizations of a jihadist nature, to commit terrorist attacks or actions.

There are circumstances that make Spain the target of international terrorism: the proximity to unstable regions such as the Sahel, the possible and growing radicalization of both first and second generation immigrants, radical Islamist claims on this country as part of Imaginary of Islam, and its decisive implication in the fight against terrorism.

The use of new technologies, with the ultimate aim of committing a traditional terrorist action or in the cyberattack mode, is a transnational problem that requires a coordinated and integrated action between different states.

However, added to the absence of global internet governance, there is another great difficulty in establishing a comprehensive strategy against this phenomenon, which is the need for technical knowledge for the effective investigation of these crimes, as well as the homologation of Procedures used to obtain information and the guarantee of its validity to support the charging in the subsequent criminal proceedings.

On the other hand, an effective counter-terrorism strategy through the use of new technologies requires police cooperation and the involvement of all relevant actors in the matter, Member States of the main International Organizations, police services, intelligence services, Cyberdefense, judges and companies providing information on technology services.

Keywords: ciberjihad, new technologies, social networks, instant messaging, recruitment, radicalization, incitement to terrorism, financing, training and planning.

1. INTRODUCCIÓN

Cuando en el año 2002 Osama Bin Laden, en una carta dirigida al Mullah Omar en Afganistán, afirmaba lo siguiente: “es obvio que en este siglo la guerra mediática es uno de los métodos más fuertes; de hecho, puede alcanzar un ratio del 90% del total de la preparación para nuestras batallas”, no podía imaginar el grado de cumplimiento de tal vaticinio. (Akil, 2010)

Las nuevas tecnologías son uno de los factores estratégicos que han sabido explotar las organizaciones terroristas con multitud de finalidades, desde el reclutamiento, la propaganda, la financiación, el adiestramiento, la incitación o provocación a realizar acciones terroristas, hasta el acopio y difusión de información con finalidad terrorista.

La determinante campaña antiterrorista que siguió a los atentados del 11S provocó un cambio de estrategia por parte de los grupos terroristas que supieron ver en el ciberespacio, el nuevo campo de batalla. El endurecimiento del control por parte de

los servicios de información y contraterrorismo sobre los sitios web que les servían de plataforma hizo que las redes sociales, entre otras, se presentasen como una nueva alternativa a los medios tradicionales online.

Al-Qaeda e ISIS son las organizaciones más activas en el uso de las nuevas tecnologías. De hecho, la primera ha tenido presencia en Internet desde los años 90 y desde el año 2011 ambas tienen cuenta en redes sociales como Twitter. El Estado Islámico (DAESH o ISIS) tiene en las redes sociales su mayor escaparate mediático. Al mismo tiempo, Al-Qaeda en la Península Arábiga (AQAP), Hezbolá, Hamas y el Frente Al-Nusra tienen también destacada presencia en Twitter.

Si bien Al-Qaeda ha sido pionera, DAESH ha superado con creces la actividad de esta en la red, dando un salto cualitativo: "mientras Al-Qaeda y sus afiliados veían internet como un lugar donde diseminar anónimamente material o realizar encuentros en un lugar oscuro, el DAESH ha aprovechado la red como un ruidoso canal en el cual promocionarse, intimidar a la gente y radicalizar a sus nuevos reclutas. Las acciones llevadas a cabo en las redes plantean, así, todo un reto para los servicios de información y contraterrorismo, que se incrementa con la proliferación de nuevas tecnologías y smartphones" (Hannigan, 2014).

Como parte de la acción contraterrorista conjunta, miles de cuentas han sido rastreadas y clausuradas, a la vez que se abrían otras nuevas, provocando una espiral que parece tener difícil solución.

Existen elementos que convierten a España en objetivo del terrorismo internacional: la relativa cercanía a regiones inestables como el Sahel, la posible radicalización de los emigrantes, tanto de primera como de segunda generación, el hecho de que los grupos fundamentalistas islámicos presenten a este país como parte del imaginario del Islam, así como su decidida implicación en la lucha contraterrorista.

El uso de las nuevas tecnologías, con la finalidad última de cometer una acción terrorista al uso o en la modalidad de ciberataque, por parte de los grupos terroristas, es un problema transnacional que exige una acción coordinada e integrada entre los diferentes estados que conforman el sistema interestatal.

Sin embargo, a la ausencia de una gobernanza global de Internet, se suma otra gran dificultad a la hora de establecer una estrategia global contra este fenómeno, que es la necesidad de conocimientos técnicos para la investigación eficaz de estos delitos, así como la homologación de los procedimientos utilizados para obtención de información y garantizar su validez para sostener la imputación en el posterior proceso penal.

Por otro lado, una estrategia eficaz contra la yihad cibernética precisa de una cooperación policial ágil e implicación de todos los actores relevantes en el asunto, Estados miembros de las principales Organizaciones Internacionales, servicios policiales, de inteligencia y del ámbito de la ciberdefensa, jueces y fiscales, compañías proveedoras de servicios de tecnologías de la información, etc. (Enríquez, 2013).

2. ÁMBITOS DE ACTUACIÓN TERRORISTA

Internet y, en concreto, las redes sociales y las aplicaciones de mensajería privada en terminales móviles se han convertido en una poderosa herramienta para los grupos

extremistas, no solo como amplificadores de sus campañas de propaganda (incluidos el reclutamiento, la radicalización y la incitación al terrorismo) sino también como medio para la financiación, adiestramiento, planificación (tanto por medio de comunicaciones secretas, como mediante la información de dominio público), la ejecución y los ataques cibernéticos. La promesa de que la participación en la yihad electrónica es tan válida como la lucha sobre el campo de batalla, ha convertido las plataformas en un terreno abonado al que es muy difícil poner coto.

2.1. PROPAGANDA

Estos, a través de mensajes, ficheros de video, revistas, presentaciones, tratados, audio virtuales o incluso juegos de video, instruyen de una manera práctica o ideológica, justifican y promueven acciones terroristas.

Desde el año 2007, con la proliferación de las redes sociales, contenidos de distribución restringida que se entregaban en mano o a través de dispositivos de almacenamiento de información, desaparecen progresivamente. Facebook, Tumblr, Twitter, Youtube, Rapidshare o Instagram, junto con los blogs, salas virtuales de charla, revistas en línea y foros, se convierten en los canales más importantes para los grupos terroristas, de difusión de manuales de fabricación de armas, guerra psicológica o captación.

Esta propaganda puede tener como audiencia objetivo los partidarios u opositores, la comunidad internacional o las víctimas de las acciones terroristas.

2.1.1. Reclutamiento

Un reclutamiento dirigido a ganar el apoyo de las personas más receptivas a la propaganda, es decir, los grupos más vulnerables y marginados de la sociedad, como son los menores. Explota los sentimientos de injusticia, exclusión o humillación.

Factores como la edad o el género son tenidos en cuenta por la propaganda terrorista además de las circunstancias sociales o económicas.

Los foros de acceso restringido constituyen un medio para que los reclutas conozcan y puedan apoyar a organizaciones terroristas, así como colaborar con estas en acciones directas.

2.1.2. Incitación

Entendida como “una estrategia que utilizan comúnmente las organizaciones terroristas para aumentar el apoyo a su causa y llamar a la acción violenta”, su criminalización presenta controversia en algunos países en cuanto a los límites del derecho a la libertad de expresión contemplados en el Pacto Internacional de Derechos Civiles y Políticos.

Como veremos en el siguiente capítulo, el artículo 5 del Convenio Europeo para la Prevención del Terrorismo, del Consejo de Europa, insta a la prohibición de la incitación a la comisión de una acción terrorista: “siendo importante diferenciar la propaganda terrorista y la incitación en sí, sin menoscabar los derechos a la libertad de expresión, asociación y religión”.

2.1.3. Radicalización

Se trata del proceso de adoctrinamiento al que sigue la transformación de los reclutas en individuos decididos a pasar a la acción violenta. Se puede considerar que el reclutamiento, la radicalización y la incitación son fases o estadios previos a la comisión de una acción terrorista.

Cualquier musulmán que decida hacer "la yihad contra el enemigo electrónicamente es considerado, en un sentido u otro, un muyahidín en tanto que reúne las condiciones de la yihad y la intención sincera y el objetivo de servir al islam y defenderlo, aun cuando está lejos del campo de batalla". Esto ha favorecido el surgimiento de la figura del "lobo solitario" o individuo que, sin pertenecer necesariamente a organización terrorista alguna, se encomienda a esta idea para cometer acciones terroristas (Weinmann, 2014).

2.2. FINANCIACIÓN TERRORISTA

La recaudación de fondos a través de las redes sociales y otras plataformas virtuales se realiza generalmente a través de cuatro vías: recaudación directa (a través del envío masivo de correos electrónicos dirigidos a simpatizantes para obtener donaciones); comercio electrónico (a través de servicios de pago en línea que ofrecen ficheros de audio o video y libros); herramientas de pago online (uso fraudulento o robo de de tarjetas de crédito, etc.) y recaudaciones a través de donaciones a instituciones benéficas legítimas o víctimas de la infiltración terrorista.

2.3. ADIESTRAMIENTO

A modo de campo de entrenamiento virtual, a través de manuales en línea, documentos de audio o video, proporcionan instrucciones, en formato multimedia, sobre cómo enrolarse en una organización terrorista, cómo fabricar explosivos, armas de fuego, etc. y cómo realizar acciones terroristas. Estos materiales, constituyen herramientas para facilitar las actividades de contrainteligencia y las técnicas de cifrado para incrementar el nivel de seguridad de las comunicaciones.

2.4. PLANIFICACIÓN

Es difícil encontrar una operación contraterrorista en la que no se haya utilizado la tecnología de Internet, especialmente en la preparación de una acción, seleccionar un potencial objetivo o realizar actos preparatorios como la reunión de información de acceso público o, en relación con el objetivo seleccionado, mapas o instalaciones, o incluso la que figura en Facebook, Twitter, YouTube, Flickr, etc.

Son comunes las "comunicaciones secretas preparatorias" con una simple cuenta de correo electrónico y un "buzón compartido". Además utilizan software para enmascarar la dirección IP o reencaminar las comunicaciones por diferentes servidores y cifrar los datos de tráfico relativos a los sitios web utilizados. Así mismo utilizan la esteganografía: el ocultamiento de mensajes, por ejemplo, en imágenes.

2.5. EJECUCIÓN

La utilización de Internet facilita la ejecución de acciones con finalidad terrorista, al reducir las probabilidades de detección y el anonimato, ofreciendo infraestructura logística. Por ejemplo, la coordinación de la ejecución de acciones terroristas concretas o las amenazas terroristas, difundidas a través de Internet para generar en la audiencia pánico o miedo.

2.6. CIBERATAQUES

Entendidos como "la explotación deliberada de redes informáticas como medio para lanzar un ataque. Suelen estar destinados a perturbar el funcionamiento normal de computadoras, servidores o la infraestructura subyacente, mediante el uso de técnicas de piratería informática, virus informáticos, programas maliciosos, flooding (saturación) y cualquier otro medio de acceso no autorizado".

3. INSTRUMENTOS JURIDICOS INTERNACIONALES Y REGIONALES DE LOS QUE ESPAÑA FORMA PARTE

3.1. ORGANIZACIONES INTERNACIONALES

El marco jurídico internacional de lucha contra el terrorismo en Internet está constituido por diversas fuentes, entre las que se encuentran las resoluciones de la Asamblea General y el Consejo de Seguridad de la ONU, los tratados, la doctrina legal y el derecho internacional consuetudinario. Las resoluciones del Consejo de Seguridad pueden imponer obligaciones jurídicamente vinculantes para todos los Estados miembros. Igualmente, la Asamblea General ha aprobado varias resoluciones sobre terrorismo que, sin embargo, no son vinculantes.

Así mismo, los Estados se obligan, jurídicamente, en base a instrumentos bilaterales o multilaterales sobre terrorismo. Es importante tener en cuenta que son los propios Estados quienes deben de enjuiciar a los responsables de actos terroristas en territorio propio, ya que los tribunales internacionales carecen, por lo general, de dicha competencia[1].

3.1.1. Resoluciones de la ONU

Ya en el año 2006, la Asamblea General, con unanimidad de los Estados miembros, aprobó la Estrategia Global contra el Terrorismo, a través de la Resolución 60/288, en la cual estos resolvieron: "condenar de una manera firme, inequívoca y sistemática el terrorismo, adoptar medidas urgentes para prevenir y combatir el terrorismo, admitir que la cooperación internacional debe ajustarse al derecho internacional y cooperar con las Naciones Unidas para luchar contra el terrorismo en Internet y utilizar, así mismo, la red como instrumento para evitar la propagación de este fenómeno".

Por otro lado, existen diversas resoluciones del Consejo de Seguridad, aprobadas en la última década, que llaman a la cooperación en esta materia. Así, las Resoluciones

1 Actualmente solo el Tribunal Especial para el Líbano (Resolución del CS de la ONU 1757/2007) tiene competencia limitada sobre el delito de terrorismo.

1373 y 1566 de los años 2001 y 2004, respectivamente, requieren a todos los Estados miembros para que adopten medidas legislativas, y de otro tipo, para luchar contra el terrorismo al mismo tiempo que les exhortan a aplicar los convenios y protocolos internacionales que más adelante se mencionan.

En la misma línea, se aprobaron las Resoluciones 1624 del año 2005 y 1963 del año 2010. La primera de ellas, relativa a la glorificación e incitación de actos terroristas por Internet, insta a todos los Estados a que adopten medidas legislativas para prohibir la inducción a la perpetración de una acción terrorista. La segunda Resolución se centra en la utilización de las nuevas tecnologías de la información y las comunicaciones para el reclutamiento, incitación, financiación, planificación y preparación de actividades terroristas.

Finalmente, la Resolución 2178, del 24 de septiembre de 2014, exhorta a los Estados miembros a adoptar todas las medidas legales necesarias para impedir la circulación de terroristas o de grupos terroristas, mediante controles fronterizos de documentos de identidad y de viaje; utilización de procedimientos de evaluación del riesgo y control de pasajeros con base empírica; agilizar el intercambio de información operativa; prevenir la radicalización y reclutamiento de combatientes terroristas extranjeros; la financiación del terrorismo y el adiestramiento en técnicas de terrorismo.

En el apartado 6 de la referida resolución, se exige a los Estados miembros que creen los instrumentos legislativos necesarios para:

"Enjuiciar y sancionar a los nacionales que se desplacen a terceros países con el propósito de cometer, planificar o preparar actos terroristas o participar en ellos, o proporcionar o recibir adiestramiento con fines terroristas. Y a los que provea o recauden fondos, o coadyuven de alguna forma, para financiar viajes y desplazamientos a otros países para cometer actos terroristas o proporcionar o recibir adiestramiento".

3.1.2. Instrumentos Universales

Actualmente, los instrumentos legales universales no definen los delitos terroristas con arreglo al derecho internacional, tan solo contemplan la obligación de los Estados a penalizar dicha figura y establecer mecanismos de cooperación internacional para enjuiciar o extraditar a los implicados en delitos de terrorismo.

No existe ningún convenio universal que trate específicamente la prevención y la represión del uso de Internet con fines terroristas. De esta forma, serán los acuerdos bilaterales y multilaterales las únicas herramientas de cooperación internacional, hasta tanto en cuanto no se logre un convenio universal general sobre la materia.

3.2. INSTRUMENTOS EN ORGANIZACIONES REGIONALES

3.2.1. Consejo de Europa

En el año 2001, en el seno de esta Organización Internacional de carácter regional, se firmó el Convenio sobre la Ciberdelincuencia, que constituye la única herramienta jurídicamente vinculante, de carácter multilateral, que aborda la comisión de actos delictivos en Internet. Este tiene como finalidad la armonización de las legislaciones de los países firmantes tanto respecto al delito cibernético como al de terrorismo, la

mejora de los mecanismos de detección, investigación y persecución de estos delitos a través de la cooperación internacional.

Así, podríamos destacar la obligación de los Estados firmantes de legislar para exigir a los proveedores de servicios de Internet la conservación de los datos durante 90 días, con carácter renovable, si media una petición de conservación de los responsables de la investigación mientras se sustancia el correspondiente mandamiento judicial. Igualmente, se confiere al registro e intervención de los datos almacenados una protección similar a las pruebas tangibles conforme a la legislación nacional correspondiente.

En el mismo sentido, exige la facilitación de los datos relativos a abonados de estos proveedores de servicios para establecer la identidad del responsable de una acción terrorista a través de Internet. Como puede ser la ubicación física de este, datos relativos al tráfico de las comunicaciones o la interceptación de las mismas de acuerdo con las respectivas legislaciones nacionales.

Finalmente, en el seno del Consejo de Europa, se elaboró el Protocolo adicional al citado Convenio, sobre la penalización de actos xenófobos o racistas, que facilita la persecución del terrorismo a través de Internet, con la finalidad de incitar a la comisión de actos violentos por motivos de raza, color, etnia, religión, etc.

Por otro lado, el Convenio Europeo para la Prevención del Terrorismo constituye un instrumento específico para este fenómeno y obliga a los países que se adhieran, miembros o no del Consejo de Europa, a tipificar como delitos la incitación pública, el reclutamiento y adiestramiento a través de Internet. De igual modo, contempla medidas de cooperación internacional como el intercambio de información.

3.2.2. Unión Europea

En la Decisión Marco del 13 de junio de 2002, 2002/475/JAI, el Consejo de la UE abordaba la armonización de la definición del delito de terrorismo en todos los Estados miembros. Debido al aumento del terrorismo de corte yihadista, se modificó en el año 2008 para introducir disposiciones específicas sobre la incitación pública, reclutamiento y adiestramiento terrorista, a través de la Decisión Marco 2008/919/JAI del Consejo de la Unión Europea, de 28 de noviembre de 2008.

Esta, en concordancia con la anteriormente citada resolución 1624 (2005) del Consejo de Seguridad de la ONU, establece un marco de referencia para la persecución de la difusión de propaganda e instrucciones para la confección de artefactos explosivos a través de la red, siempre y cuando tengan como finalidad la comisión de actos terroristas.

A raíz de los atentados de París de enero de 2014, y más recientemente de los de noviembre de 2015, se han aprobado, en el seno de la UE, una serie de medidas para luchar contra este concreto fenómeno:

1. “Una nueva Decisión Marco que crea un marco legal para la cooperación contra el terrorismo y la Estrategia de Seguridad Interior.
2. Desarrollo del SIS (Schengen Information System), sistema de intercambio de información, y del Mecanismode Protección Civil.

3. Creación de la RAN (Radicalisation Awareness Network), red de expertos multidisciplinar que identifica casos de buenas prácticas para prevenir la radicalización en los entornos sociales identificados como de riesgo.
4. Reforzamiento de la cooperación entre Europol y otras agencias europeas y mejora del intercambio de información sobre la compraventa ilegal de armas.

La propuesta más importante es la culminación de la adopción de un registro PNR (Passenger Name Record), para mejorar el control de los pasajeros que ingresan o salen de la UE" (Narrillos, 2015).

3.2.3. España

A nivel nacional existe un marco en forma de acuerdo entre los dos principales partidos nacionales, y a los que se han ido sumando otros, ante la necesidad de afianzar la unidad de los demócratas frente al terrorismo. Se trata del "Acuerdo para afianzar la unidad en defensa de las libertades y en la lucha contra el terrorismo", que ha sido reeditado el pasado 14 de noviembre tras los atentados del 13 del mismo mes en París.

Este contemplaba, como medidas principales a adoptar, las modificaciones legislativas penales o el Plan Estratégico Nacional de Lucha contra la Radicalización Violenta (PEN-LCRV), aprobado por Acuerdo de Consejo de Ministros el 30 de enero de 2015, que relaciona tres ámbitos de actuación, interno, externo y ciberespacio, coherente con la Estrategia de Seguridad Nacional Española aprobada en 2013, y tres áreas funcionales según el momento en que debe hacerse frente al fenómeno de la radicalización: antes, durante y después.

Como se ha mencionado anteriormente, en virtud de la Resolución 2178, del Consejo de Seguridad de las Naciones Unidas, se ha adaptado la legislación penal nacional a través de la LO 2/2015 de 31 de marzo de 2015.

Según el Grupo de Estudios en Seguridad Internacional, "esta reforma constituye un gran paso para la prevención de la difusión del terrorismo yihadista a través de redes sociales, entre otros medios, tipificando tanto la difusión de ideas incitadoras como el adiestramiento en técnicas para la comisión de cualquier delito de terrorismo. También supone un importante apoyo legislativo la penalización de los desplazamientos a territorios controlados por organizaciones o grupos terroristas, para recibir adiestramiento o adoctrinamiento, tipificándolos como delito".

Las modificaciones derivadas de esta Resolución afectan a los delitos de terrorismo contenidos en los artículos 571 al 580 del Código Penal, destacando la introducción expresa de la configuración de los delitos informáticos como delitos de terrorismo cuando se cometan con finalidad terrorista. "Se tipifica como delito el que, con esta finalidad de adiestrarse, tenga en su poder documentos, archivos o acceda de forma habitual a servicios de comunicación vía internet o electrónica cuyos contenidos sean idóneos para incitar a la incorporación a organizaciones o grupos terroristas o a colaborar con cualquiera de ellos".

Igualmente, "en relación a los delitos de enaltecimiento o actos de humillación, descrédito o menosprecio a las víctimas del terrorismo, cabe la adopción judicial de medidas cautelares en el caso de que dichos delitos se cometan mediante servicios o contenidos accesibles a través de internet o de servicios de comunicaciones

electrónicas. Se podrá ordenar la retirada de los contenidos, la supresión de los enlaces y la prohibición de acceso a dichos contenidos ilícitos".

Por otro lado, la reciente Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, constituye un marco de referencia para hacer frente a esta amenaza a través del ciberespacio, "considerando la Seguridad Nacional como un objetivo compartido por las diferentes administraciones, estatal, autonómica y local, los órganos constitucionales, en especial las Cortes Generales, el sector privado y la sociedad civil, dentro de los proyectos de las organizaciones internacionales de las que formamos parte".

Otra de las novedades en esta materia es la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

Entre las importantes novedades procesales que contiene destaca la adaptación a las formas de delincuencia ligadas al uso de las nuevas tecnologías. Así:

- "Toda medida de intervención deberá responder al principio de especialidad: la actuación de que se trate deberá tener por objeto el esclarecimiento de un hecho punible concreto, prohibiéndose las medidas de investigación tecnológica de naturaleza prospectiva.
- Las medidas de investigación tecnológica deben satisfacer los principios de idoneidad, excepcionalidad, necesidad y proporcionalidad, cuya concurrencia debe encontrarse suficientemente justificada en la resolución judicial habilitadora.
- Se autoriza la intervención y registro de las comunicaciones de cualquier clase que se realicen a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual.
- Se establece un plazo de tres meses como duración máxima inicial de la intervención, hasta un máximo de 18 y se regula el registro de dispositivos informáticos de almacenamiento masivo y el registro remoto de equipos informáticos.
- Para asegurar la autenticidad e integridad de los soportes puestos a disposición del juez, se impone la utilización de un sistema de sellado o firma electrónica que garantice la información volcada desde el sistema central.
- Por último, se regula la figura del agente encubierto informático, que requiere autorización judicial para actuar en canales cerrados de comunicación y que a su vez, requerirá una autorización especial para intercambiar o enviar archivos ilícitos por razón de su contenido en el curso de una investigación".

3.3. PROBLEMÁTICA JURÍDICA Y PROCESAL ENTRE MARCOS NORMATIVOS

En este apartado, se pretende poner de manifiesto los problemas derivados de los diferentes enfoques legales a nivel internacional que dificultan la persecución del terrorismo yihadista en Internet. Teniendo en cuenta que no solo basta con adaptar la legislación nacional a esta concreta amenaza, sino que es necesaria una armonización internacional, debido al carácter transnacional de la misma.

Actualmente y debido a la dimensión de la evolución de la amenaza en los últimos meses, los Estados están legislando a marchas forzadas en este ámbito, pero todavía muchos de ellos carecen de legislación específica en el uso de Internet con fines terroristas.

Sin embargo, a nivel internacional, no existe un instrumento amplio y vinculante que establezca normas definitivas sobre la regulación de las actividades en Internet. Por ello, la mayoría de países han optado por lidiar con el fenómeno mediante la combinación de leyes penales generales y específicas sobre terrorismo y ciberdelincuencia, ya existentes en sus respectivos ordenamientos. Así, las diferentes fiscalías, hacen uso de las disposiciones normativas que se adaptan mejor al caso.

Máxime, ante la ausencia de una definición universalmente aceptada de terrorismo como la que existe acerca de la pornografía infantil. (Conway, 2007).

3.3.1. Ámbito Penal

Ante la ausencia de imposición, por parte de los instrumentos internacionales contra el terrorismo, de la obligación de legislar específicamente contra el uso de Internet con fines terroristas, los Estados han optado por recurrir a sus respectivos códigos penales, además de invocar los instrumentos universales que tratan la amenaza.

El principal problema radica en la diferente o ausente penalización de conductas o figuras relacionadas con el terrorismo yihadista en muchos países donde se encuentran ubicados los servidores o los proveedores de servicios de Internet.

Sin este requisito de la doble incriminación, muchas investigaciones y procesos penales iniciados en un Estado se frustran. Por tanto, es fundamental que cuando se tipifiquen estas conductas se utilicen figuras delictivas lo más similares posible para evitar diferentes interpretaciones.

3.3.2. Ámbito Procesal

Los instrumentos jurídicos universales citados en el punto uno, prevén la extradición, la asistencia judicial recíproca, la remisión de actuaciones penales y traslado de las personas condenadas, la ejecución recíproca de sentencias, el embargo preventivo y decomiso de activos. Sin embargo, la incompatibilidad de los diferentes sistemas penales ha puesto en evidencia, en la práctica, que las solicitudes de asistencia judicial recíproca o de extradición habían sido rechazadas o ejecutadas con demora por no satisfacer, entre otros, el requisito de la doble incriminación.

El primer obstáculo surge en relación al intercambio de información confidencial entre los diferentes países. Los órganos jurisdiccionales que compartan datos reservados exigen que sus destinatarios mantengan las debidas garantías de la que gozan en sus respectivos países.

Otro, es el concepto de soberanía de los Estados. En algunos casos estos pueden percibir una investigación en su territorio como una injerencia. Tal es el caso del registro a distancia de un ordenador ubicado en otro país. Otro aspecto controvertido es la retención y entrega de la información vinculada a actividades realizadas por Internet por una persona

relacionada con el terrorismo. Así como información sobre cuentas bancarias, tarjetas de crédito, información sobre el uso por parte de esta de servicios de comunicaciones por Internet como el correo electrónico, Skype, VoIP, redes sociales u otros sitios web.

Uno de los problemas principales es la ausencia de un marco internacional o convenio sobre la retención de estos datos por parte de los proveedores de servicios de Internet. A nivel internacional, no existe ningún plazo establecido de referencia, por lo que es muy complicado llegar a tiempo para salvaguardar la información cuando se trate de investigaciones que afecten a más de un país[2].

Cuestión también importante es la observancia de los requisitos probatorios de los sistemas legales de los países afectados. La información proporcionada a través de la cooperación policial, con métodos de registro, vigilancia e interceptación, encubiertos o intrusivos, altamente especializados debe ser coherente con la jurisdicción que finalmente entenderá del asunto. Por ejemplo la cadena de custodia de la intervención física de los ordenadores para análisis forense o los informes periciales realizados por expertos en la lucha contraterrorista.

Otra cuestión que plantea problemas es la competencia sobre el delito en cuestión, cuando el terrorista está ubicado en un país pero utiliza, para la su comisión, sitios de Internet o servicios de proveedores ubicados en otro. En este caso, ante la ausencia de normas vinculantes en el derecho internacional para dirimir los conflictos de competencia, los Estados se basan en cuestiones como la nacionalidad de este, el lugar de la comisión o el lugar donde se encuentran los testigos y las pruebas para reivindicar su competencia.

Por otro lado, muchos países condicionan la cooperación en esta materia a la existencia de tratados internacionales o, al menos, de reciprocidad con el país requirente, en materia de asistencia judicial recíproca y extradición.

Finalmente, otro gran obstáculo existente en la persecución del terrorismo y del uso de las nuevas tecnologías con el mismo fin son las legislaciones nacionales de protección de datos y de la privacidad.

4. RESPUESTA POLICIAL: INSTRUMENTOS DE COOPERACIÓN POLICIAL INTERNACIONAL Y PROCEDIMIENTOS DE INVESTIGACIÓN. CONTRIBUCIÓN MILITAR

4.1. COOPERACIÓN POLICIAL INTERNACIONAL

Ante la ausencia de un instrumento universal que aborde el uso de las nuevas tecnologías con fines terroristas, para facilitar la cooperación judicial y policial internacional en esta materia, se hace necesario recurrir a otros instrumentos no específicos, ya existentes, en el ámbito de las organizaciones de las que España forma parte o con los países con que mantiene acuerdos multilaterales o bilaterales.

2 Tan sólo la UE ha establecido tal obligación, de 6 meses a 2 años, pero existe inseguridad jurídica mientras no haya un período de retención estándar.

4.1.1. Instrumentos de cooperación no específicos

Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional: Se trata de la principal herramienta para la cooperación entre Estados en materia de delincuencia organizada pero que, dadas las características que reúnen las organizaciones terroristas, es posible su aplicación a los casos de terrorismo internacional.

Convenio sobre la Ciberdelincuencia y otros: Contiene mecanismos de cooperación en materia policial y judicial, como pueden ser la comunicación oficiosa de información entre Estados, miembros o no miembros del Consejo de Europa, adheridos.

Además de este, el Convenio Europeo para la Prevención del Terrorismo del Consejo de Europa, el Convenio Europeo sobre Extradición, el Convenio Europeo sobre cooperación judicial en materia penal y el Acto 2000/C 197/01, de 29 de mayo de 2000, del Consejo de la UE, relativo a la asistencia judicial en materia penal entre Estados de la UE, podrían ser de aplicación para la cooperación internacional en materia de terrorismo internacional que tenga relación con el uso de Internet.

4.1.2. Otros instrumentos de cooperación

Orden de Detención Europea: Establece, dentro del marco Schengen, la obligatoriedad para los Estados de la UE de detener y trasladar a un presunto terrorista al Estado requirente, en base al principio de reciprocidad. Esta incluye a los propios nacionales cuando el hecho ha sido cometido en otro país miembro.

Orden Europea de Investigación (OEI). Consiste en un procedimiento simplificado para obtención y remisión, establecido en virtud de la Directiva del Parlamento Europeo y del Consejo 2014/41/CE, de documentos, objetos, datos de usuarios de Internet, etc. que puedan servir de elementos de prueba.

Red 24/7 del Consejo de Europa: Establecida en virtud del artículo 35 del Convenio sobre la Ciberdelincuencia del Consejo de Europa, establece la disponibilidad de contactos, las 24 horas del día los siete días de la semana, para casos de ciberdelincuencia.

En el seno del Consejo de Europa se creó, también, el Comité Especial de Expertos sobre la evaluación de medidas contra el blanqueo de dinero y financiación del terrorismo.

Plan de acción de la Unión Europea: Centro de Ciberdelincuencia: Los Estados miembros encomendaron a la Comisión Europea y a Europol la tarea de crear un Centro Europeo de Ciberdelincuencia. Este se dedica a la lucha contra las organizaciones criminales que cometen ciberdelitos graves.

A nivel europeo, los diferentes cuerpos policiales colaboran en mejorar las técnicas y procedimientos de investigación a través de internet, desarrollando incluso herramientas propias que se puedan emplear por todos los investigadores.

4.1.3. Instrumentos de cooperación internacional entre agencias y cuerpos de seguridad

Grupo Egmont de unidades de inteligencia financiera: Se trata de un organismo internacional cuya finalidad es la promoción y optimización de la cooperación de las

unidades de inteligencia financiera en la persecución del blanqueo de capitales y financiación del terrorismo.

Organización Internacional de Policía Criminal. (INTERPOL): Para el intercambio y análisis de información entre los países miembros, a través de su sistema I-24/7 y el programa de ciberdelincuencia para coordinar las operaciones internacionales, prestar asistencia en investigaciones, asistencia en caso de ciberataques, etc.

Oficina Europea de Policía (EUROPOL): Responsable de reforzar la cooperación entre las Fuerzas y Cuerpos de Seguridad de los Estados miembros de la UE en materia de terrorismo y delincuencia organizada, a través de Internet. Proporciona: base de datos sobre ciberdelincuencia**,** programa de evaluación de la amenaza de la delincuencia organizada por Internet, incluido terrorismo, y los ataque a redes electrónicas (iOCTA), sistemas de denuncias on-line de delitos cometido por Internet (ICROS) y el Foro de Expertos Forenses (iFOREX).

Europol ha puesto en marcha un nuevo equipo policial especialmente formado para bloquear y cerrar todas aquellas cuentas en plataformas sociales que estuvieran vinculadas con el terrorismo islámico (Casciani, 2015). También se ha puesto en marcha el Centro Europeo Contra el Terrorismo (ECTC), al mando de un Coronel de la Guardia Civil, con la finalidad de mejorar el intercambio de información tanto operativa como estratégica en el ámbito de esta amenaza.

Eurojust: Como unidad de cooperación judicial de la UE, en colaboración con Europol, promueve el intercambio de información entre las diferentes autoridades judiciales en investigaciones y enjuiciamientos relacionados con el terrorismo, emisión y ejecución de órdenes de detención europea, etc.

Una herramienta útil en este ámbito es el Terrorism Convictions Monitor (TCM)[3], es un informe interno de Eurojust que, entre otras cuestiones, facilita a los miembros de la justicia ejemplos de sentencias y de interpretación de la legislación de la UE contra el terrorismo. Especialmente útil en el tratamiento desde el punto legal de los foreign fighters.

Cooperación oficial y oficiosa: A pesar de la existencia de estos instrumentos mencionados, es necesaria para una cooperación internacional eficaz la existencia de una autoridad central que asuma esa responsabilidad, con capacidad legal, autonomía e iniciativa suficiente para liderar la coordinación entre autoridades policiales, servicios de inteligencia (incluida la financiera), autoridades judiciales e incluso aquellas unidades pertenecientes al ámbito de la ciberdefensa. Con procedimiento claros y simplificados que incluyan mecanismos oficiales y oficiosos.

Aunque los canales oficiales ofrecen mayor garantía en cuanto al éxito de las investigaciones y enjuiciamiento de este tipo de delitos, los procedimientos oficiosos son mucho más ágiles y exigen menos burocracia. Y dado que el factor tiempo es fundamental para la disponibilidad de datos digitales, este será el medio más habitual, principalmente a través de oficiales de enlace (en cuerpos policiales extranjeros o Agregadurías de Interior) e investigaciones conjuntas (equipos conjuntos de investigación de duración limitada en el seno de EUROPOL).

3 Implementado por la Decisión 2005/671/JAI del Consejo de la Unión Europea.

4.2. PROCEDIMIENTOS Y HERRAMIENTAS DE INVESTIGACIÓN

Las actuales investigaciones de la actividad terrorista yihadista en Internet se basan en una combinación de métodos de investigación tradicionales y los ideados específicamente en relación con las pruebas digitales, que exigen estar familiarizados con las técnicas especializadas de investigación en un entorno virtual.

4.2.1. Comunicaciones por Internet

Telefonía de voz por Internet (VoIP): A través de estas aplicaciones los terroristas pueden comunicarse en tiempo real, incluyendo conversaciones a través de video o texto, y permiten compartir ficheros. Destacan los proveedores de servicios VoIPSkype y Vonage, etc., los cuales convierten el sonido analógico en formato digital comprimido con lo que no requieren de un gran ancho de banda.

Las dificultades en la investigación se deben a que la facturación se realiza en base al volumen de paquetes de datos transmitidos en lugar de las señales analógicas como se hace con las llamadas tradicionales telefónicas, con lo que se hace más complicada la determinación de hora de llamada o ubicación de los usuarios. Si, además, las llamadas se realizan a través de redes punto a punto (P2P) o mediante el cifrado de datos de llamada, la dificultad es aún mayor.

Sin embargo, el volumen del tráfico de datos en un momento dado, así como la dirección IP, dirección electrónica o los datos de pago del usuario proporcionados por el proveedor de servicios de Internet, pueden servir para la identificación de este.

Correo electrónico: Proporciona un medio encubierto de comunicación. Un correo electrónico estándar se compone de encabezado del sobre, encabezado del mensaje, cuerpo del mensaje y ficheros adjuntos.

El encabezado del sobre suele proporcionar información sobre los servidores por los que ha pasado el mensaje hasta su destino y la información sobre la dirección IP del remitente. Esta es más difícil de manipular que la del encabezado del mensaje.

Para reducir (o eliminar) la posibilidad de detección, los terroristas suelen utilizar el procedimiento de comunicación a través de mensajes no enviados, accesibles desde la carpeta de borrador y al que pueden acceder múltiples destinatarios con una contraseña compartida de acceso a la cuenta. Si además utilizan un terminal de acceso público, como un cibercafé, las posibilidades de identificación de estos se reducen.

Así mismo, emplean técnicas de anonimato ocultando la dirección IP del remitente o utilizando servidores de correo que mantienen el anonimato, sesgando la información de identificación del encabezado del sobre.

Para intercambiar información de promoción terrorista, emplean software de esteganografía Camouflage para ocultar datos dentro de imágenes en formato JPEG y GIF y software de WinZip para cifrar ficheros, que se remiten adjuntos a las comunicaciones por correo electrónico.

Servicios de mensajería en línea y chats (salas de charla): Los primeros son un medio de comunicación bilateral, mientras que los segundos lo son para un grupo

de personas. La inscripción para el uso de estos servicios se basa en información no verificada que proporciona el propio usuario.

Aunque algunos proveedores de servicios registran la dirección IP de acceso, no guardan, generalmente, la información intercambiada durante una sesión y para su recuperación posterior será necesario el análisis forense del disco duro de al menos uno de los usuarios.

Las salas de charla en línea a través de contraseña, que son frecuentemente utilizadas por los terroristas y simpatizantes, ofrecen mayores posibilidades de obtención de pruebas documentales, incluso la infiltración en las mismas, a través de la figura del agente encubierto, con la limitación de no incurrir en la comisión de la infracción penal de inducción al delito.

Redes de intercambio de ficheros y almacenamiento en nube: Los más utilizados son los sitios web Fileshare, Rapidshare o Dropbox, que proporcionan la posibilidad de cargar, compartir y acceder a ficheros multimedia a través de la red. Estas permiten el cifrado y el anonimato mediante la tecnología P2P y el Protocolo de Transferencia de Ficheros (FTP).

En el marco de una investigación, alguna de estas redes puede dejar rastro de transferencias de efectivo o pagos, útiles con fines de identificación de usuarios.

Con respecto a la computación en nube, proporciona acceso remoto a programas y datos almacenados o ejecutados en los servidores de datos de terceros. Esta permite el almacenamiento, compartición y distribución de documentación en línea.

Al reducir la cantidad de información almacenada localmente en los dispositivos físicos, dificulta la recuperación de pruebas con fines investigativos, que aumenta si, además, los servidores de datos están ubicados en otro país.

Cifrado de datos y anonimato: A través de un algoritmo matemático y una clave de cifrado pueden proteger la información del conocimiento de terceros. Con un equipo físico, un software o una combinación de ambos son capaces de cifrar datos “en reposo”, contenidos en discos duros de los ordenadores, unidades externas de memoria o smartphones, y los datos “en tránsito” a través de Internet, como los anteriormente mencionados telefonía VoIP y correo electrónico.

“Los más habituales son los programas informáticos WinZiP, Truecrip y Pretty Good Privacy (PGP) para la protección de contraseñas y para el cifrado o esteganografía el Camouflage. También hacen uso del software Detekt que identifica malware de vigilancia sobre sus actividades en la Red.

Otra técnica que utilizan para ocultar la identidad de los usuarios es la de ocultación de la dirección IP de origen, usurpar la de otro terminal o redirigir la información a una dirección IP oscurecida”.

Una de las maneras de salvar esta dificultad es la aprehensión del equipo informático encendido y con los ficheros abiertos, salvando las claves criptográficas. Para ello, es necesario recurrir a técnicas tradicionales, como el seguimiento de la actividad del sospechoso para elegir el momento idóneo de la detención.

Redes inalámbricas (Wi-Fi): que permiten el acceso a Internet con ordenador u otro dispositivo (teléfono móvil, tabletas, etc.) a través de una señal de radio. Pueden facilitar el acceso a través de contraseña o abierto. El acceso anónimo a estas permite a los terroristas desvincular su actividad en Internet con sus datos identificativos.

En la actualidad existen empresas proveedoras de servicios, como la española FON, que permite que los usuarios inscritos compartan su ancho de banda de red wi-fi con otros abonados en cualquier parte del mundo, a través de una aplicación que localiza esas redes.

Por tanto, las dificultades de investigación son considerables, tanto en lo que respecta a la posibilidad de interceptación de las comunicaciones como de la localización de los transmisores.

Red TOR (The Onion Router): Conocida como la red oscura en la que los mensajes intercambiados no revelan la dirección IP de los usuarios. Los mensajes no viajan entre iguales (Peer to Peer, P2P), sino a través de una serie de "routers cebolla" a modo de encaminadores de los mismos, cedidos por diferentes organizaciones o individuos con ancho de banda suficiente. (Gellman y Rich, 2013).

4.2.2. Investigación Tipo

Enfoque sistemático de las investigaciones: Internet ofrece herramientas útiles, como datos y servicios disponibles, que se pueden emplear en una investigación tipo contra el terrorismo yihadista a través de la red.

La necesidad de establecer un procedimiento sistemático de investigación a través de Internet, ha llevado a INTERPOL y EUROPOL, con la participación de la Universidad de Dublín y su Máster en Informática Forense y Ciberdelincuencia, a elaborar un protocolo para este fin, ya llevado a la práctica por muchos Estados miembros, y que establece los hitos básicos para realizar este tipo de investigaciones.

Valor identificativo de una dirección IP: Toda comunicación de Internet tiene asociada una IP (Protocolo Internet) que identifica la red y el dispositivo desde el cual se ha realizado ese acceso. Las direcciones IP pueden ser dinámicas, facilitada por un proveedor de servicios temporalmente y para una sesión en línea, o estáticas, como las direcciones de los sitios web.

En las primeras de ellas, se puede identificar la región o país desde donde un ordenador se conecta a Internet y a través del correspondiente mandamiento judicial, y previo requerimiento para la conservación de los datos digitales hasta que se libere este, se puede solicitar a un proveedor de servicios de Internet que identifique la cuenta de un abonado que, en un momento dado, estaba vinculada a una determinada dirección IP.

En las investigaciones relacionadas con sitios web es necesario identificar qué dirección IP estática corresponde al nombre del dominio en cuestión. Para ello, se utilizan aplicaciones basadas en un protocolo TCP (Protocolo de Control de Transmisión) de petición respuesta como who.is o nslookup. Sin embargo, la información registrada es la que previamente ha proporcionado el titular o puede encontrarse el dominio arrendado a otro titular diferente.

Es importante tener en cuenta que toda actividad investigadora puede a su vez ser monitorizada por terceros. Por ello, no debe realizarse desde equipos oficiales.

Aplicaciones especializadas de investigación: Existen diversas aplicaciones de búsqueda especializadas, que pueden ser utilizadas con fines identificativos si se dispone de una adecuada formación técnica. Por ejemplo, “Ping”, la cual permite conocer si un ordenador está conectado a Internet en un momento dado, a través del envío de una señal o “Traceroute”, que facilita la ruta entre dos ordenadores conectados en red permitiendo determinar así su ubicación física.

Existen otros programas que, con las limitaciones legales de cada país, permiten el acceso a dispositivos e interceptación de las comunicaciones. Son los denominados caballos de Troya, que sirven para la obtención de información o el control remoto de un ordenador, una vez se ha introducido en este.

Por otro lado, los capturadores de teclado (hardware o software), pueden obtener información de la actividad de un teclado, como pueden ser las contraseñas de acceso, comunicaciones o actividad en un sitio web. Por su parte, los “Sniffers” o rastreadores de paquetes de datos, permiten la obtención de información de la fuente y el contenido de las comunicaciones.

Preservación y recuperación de datos: Para su uso con fines probatorios, la recuperación de datos digitales almacenados deben realizarse respetando las técnicas forenses que permitan su admisibilidad en juicio y como en cualquier investigación, con escrupuloso respeto de la cadena de custodia.

En cuanto a la preservación de datos, si se interrumpe el suministro eléctrico de un ordenador los datos volátiles de los discos de almacenamiento y memoria RAM pueden verse alterados, perdiéndose información sobre usuarios, contraseñas o mensajes instantáneos. Sin embargo, los datos no volátiles almacenados en discos duros, unidades de memoria portátiles, dispositivos de almacenamiento flash y discos de compresión (discos ZIP), no se ven afectados por esta circunstancia.

En el documento publicado por UNODC: “Manual de buenas prácticas para incautarse de pruebas electrónicas”, se incluye una guía de este proceso.

Con respecto a los teléfonos inteligentes, tabletas, etc., se utiliza el mismo procedimiento pero debe evitarse el apagado del dispositivo por el requerimiento posterior de contraseña o pérdida de datos.

Los exámenes que se realicen sobre los datos deben de realizarse sobre copias de los elementos de prueba originales, utilizando herramientas forenses como EnCase, de la empresa Guidance Software o FTK (Forensic Tool Kit). Existen otros programas gratuitos y sería conveniente utilizar dos diferentes para crear duplicados y asegurar la preservación de datos.

Validación de la autenticidad de las pruebas digitales: Para el enjuiciamiento de un caso de uso de Internet con fines terroristas es imprescindible garantizar la integridad de las pruebas digitales y, especialmente, la cadena de custodia.

EnCase, por ejemplo, crea una imagen duplicada de los datos y analiza el dispositivo para capturar ficheros ocultos o borrados. También crea y asigna un identificador

único (valor hash) a las pruebas digitales, con la finalidad de validar su autenticidad. La coincidencia de los valores hash confirma la no manipulación de estas y permite trabajar sobre los datos de la copia con validez judicial.

Informes periciales de inteligencia: La información obtenida acerca de la actividad terrorista, en general, y en Internet, en particular, puede servir de punto de partida para el inicio de una investigación policial y posteriormente judicial, una vez trabajada y elaborada, generando el correspondiente informe de inteligencia.

Además, puede servir de prueba en un posterior juicio en determinados ordenamientos jurídicos, entre los que se encuentra el español, convirtiéndose así en un informe pericial de inteligencia y los funcionarios policiales que lo redactan se convierten, por tanto, en peritos de inteligencia.

En la mayoría de Estados existe la dicotomía entre la confidencialidad de la identidad de la fuente, informador o colaborador y el derecho de los procesados a un juicio justo y que se respete el principio de contradicción o de conocer y rebatir las pruebas que se presenten en su contra. Y más a tenor de la escasa protección que, legislaciones como la española, otorgan al testigo protegido.

En otros muchos países la inteligencia procedente de fuentes anónimas no es admisible como elemento de prueba salvo si es complementada con otras pruebas o corroborada por funcionarios policiales de un determinado rango.

4.2.3. Colaboración con otros actores

Fuerzas Armadas y Centro Nacional de Inteligencia: En el ámbito de las ciberamenazas se plantean las siguientes dudas: por un lado, qué constituye un acto de ciberguerra y, por otro, la atribución de la responsabilidad del mismo, con lo cual queda la duda de qué organización debería tomar la iniciativa cuando ocurren cibereventos y no está claro quién está detrás de ellos. “Si se trata de una cuestión de seguridad nacional o un asunto militar dependiendo de si detrás de ellos se encuentran delincuentes, hackers, terroristas o estados paria. La evidencia necesaria para probarlo ante un tribunal exigirá mucho más”. (Caro, 2010)

Más allá de la cibercriminalidad, en el ámbito de la ciberdefensa, se precisa una definición más clara de qué se entiende por acto de ciberguerra y quién es el responsable del mismo. Mientras no se establezca una cooperación internacional adecuada en ciberinvestigación, la capacidad de atribuir un ciberataque a un autor concreto será difícil. (Caracuel, 2002)

Teniendo en cuenta el tratamiento que desde el Gobierno de la nación se ha dado al terrorismo yihadista, a través del mencionado “Acuerdo para afianzar la unidad en defensa de las libertades y en la lucha contra el terrorismo”, parece evidente que se ha basado eminentemente en un enfoque penal, que implica especialmente a Fuerzas y Cuerpos de Seguridad, Jueces y Fiscales.

No obstante, pese a que la investigación de esta amenaza desde el punto de vista de la seguridad interior compete a las FCSE, bajo la coordinación del CITCO, en la práctica, Fuerzas Armadas y CNI colaboran, desde el punto de vista técnico y de intercambio

de información, para poner a los terroristas a disposición de las autoridades judiciales nacionales[4].

Sector privado: la colaboración por parte de estos es fundamental para una respuesta oportuna y eficaz contra el terrorismo yihadista y el uso que sus miembros hacen de Internet. A pesar de que ya colaboran de facto, tienen la obligación moral de hacer más. (Ben Solomon, 2014)

Proveedores de servicios de Internet juegan un papel crucial en la conservación y cesión de datos digitales y en el rigor con el que los exigen a sus usuarios para hacer uso de sus servicios.

Por otro lado, los sitios web o plataformas que hospedan contenido generado por los usuarios, como YouTube, con casi ocho millones de usuarios al mes, puede hacer de barrera a los contenidos de corte yihadista al permitir que los usuarios denuncien aquellos que inciten, promuevan, etc. Lo mismo se podría decir de Twitter o facebook. (Chimbelu, 2015)

Conway (2007) sostiene que los buscadores de Internet (Google, Yahoo, etc.) constituyen un puente entre los contenidos de Internet y el usuario, por tanto, estos pueden bloquear y eliminar los resultados de búsqueda relacionados con posibles organizaciones terroristas.

Por otro lado, existen servicios de monitorización como Search for International Terrorist Entities (SITE), que funcionan como un servicio de inteligencia y recibe sus ingresos de suscripciones. O Internet Haganah, que detecta y bloquea el acceso a contenidos extremistas islámicos y se financia por aportaciones de una red de voluntarios. (Eunjung, 2005).

5. CONCLUSIONES

Es evidente que la Comunidad Internacional se encuentra, más que nunca, bajo la amenaza del terrorismo yihadista quién, con la promesa de que la participación en la yihad electrónica es tan válida como la lucha sobre el campo de batalla, ha encontrado en las nuevas tecnologías su mejor instrumento para llegar a los jóvenes, como principal audiencia objetivo.

A marchas forzadas los gobiernos y las principales empresas se replantean la necesidad de monitorizar dichas redes, con la clara finalidad de evitar la radicalización de los jóvenes y prevenir ataques terroristas. Lejarza (2015) defiende que la tarea se presenta complicada, debido a la pericia que han alcanzado dichas organizaciones para evadir cualquier intento de control por parte de los servicios de inteligencia.

Además, y pese al carácter transnacional de este terrorismo, no existe ni una definición oficial del término terrorismo, ni ningún convenio universal que aborde espe-

4 Destacan los Comités Especializados de Ciberseguridad y de Situación bajo la dependencia directa del Consejo de Seguridad Nacional. Cada país tiene sus CERT (Equipo de Respuesta a Emergencias Informáticas) para hacer frente a los ciberataques (que pueden ser de origen terrorista). En OTAN, existe el NATO Computer Incidents Response Capability Technical Centre (NCIRC-TC). A nivel europeo la European Union Agency for Network and Information Security (ENISA) intercambia información de interés para la prevención de ciberataques.

cíficamente la prevención y la represión de este asunto desde un perspectiva global, más allá de diversas resoluciones del Consejo de Seguridad de la ONU, que obliga a los Estados miembros a cooperar sin reservas en esta materia.

Ante la ausencia de una legislación armonizada en materia de Ciberseguridad, se han elaborado convenios o convenciones de carácter regional, en el seno del Consejo de Europa o la Unión Europea, que pretenden regular y uniformar criterios con más o menos acierto. Esto ha provocado que los Estados hayan adoptado soluciones "ad hoc", aplicando una combinación de leyes penales generales con otras específicas de ciberdelincuencia y contraterrorismo.

No obstante, a raíz de los recientes atentados de París y Bruselas, en el seno de la UE ha habido avances importantes, destacando, entre otros, medidas como la adopción del registro y control de pasajeros, Passenger Name Record (PNR), con origen o destino en la UE.

España ha sido de los países que más medidas ha adoptado durante el productivo, desde el punto de vista legislativo, año 2015, en relación a la prevención del impulso del terrorismo yihadista a través de redes sociales, comunicaciones electrónicas o creación de páginas web o foros, "penando tanto la difusión de ideas incitadoras como el adiestramiento en técnicas para la comisión de cualquier delito de terrorismo. Destacando, entre otras, la introducción expresa de la configuración de los delitos informáticos como delitos de terrorismo".

Ya en el ámbito penal y procesal es donde mayores disfunciones se evidencian por la incompatibilidad de los diferentes sistemas penales internacionales. Así, las solicitudes de asistencia judicial recíproca o de extradición se rechazan sistemáticamente o se ejecutan con demora por no satisfacer, entre otros, el requisito de la doble incriminación o del respeto a la cadena de custodia correspondiente.

Además, la ausencia de un acuerdo o convenio sobre los plazos de conservación de los datos por parte de los proveedores de servicios de Internet, a nivel internacional, dificulta recuperar la información en investigaciones que afecten a más de un país. Los métodos de registro, vigilancia e interceptación o los informes periciales deben reunir los requisitos procesales de países con muy diferentes niveles de exigencia en este ámbito.

Finalmente, se carece de normas internacionales vinculantes para dirimir las cuestiones de competencia cuando el terrorista está ubicado en un país y el servidor de Internet en otro distinto, o por el diferente grado de protección que cada país otorga a los datos personales y la privacidad, principal obstáculo para la investigación.

En el ámbito de la respuesta a este fenómeno, se hace patente la necesidad de incrementar la formación, especialmente en investigación e informática forense, y continuar con la colaboración, ya iniciada, con universidades y expertos. Los procedimientos de investigación precisan de una normalización internacional. Estos se basan en una combinación de métodos tradicionales con otros técnicos que se encuentran disponibles en la propia Red pero que no están homologados y su validez jurídica se basa en el informe técnico pericial del perito correspondiente.

Por todo ello, las herramientas legales, de cooperación policial y procedimientos técnicos de investigación, debido a la multitud de actores implicados, la dificultad de

coordinación y la rapidez con que evolucionan las nuevas tecnologías y procedimientos utilizados por las organizaciones terroristas hacen que la capacidad de respuesta sea inferior a la de la amenaza.

BIBLIOGRAFÍA

Akil A. (2010). The virtual Jihad: An Increasingly Legitimate Form of Warfare. Combating Terrorist Center. Extraído el 06 de noviembre de 2015 de: https://www.ctc.usma.edu/posts/the-virtual-jihad-an-increasingly-legitimate-form-of-warfare.

Ambos K. (2012). Creatividad judicial en el Tribunal Especial para el Líbano: ¿Es el terrorismo un crimen internacional? Revista de derecho penal y criminología. Universidad Nacional de Educación a Distancia. 3ª Época, nº 7, p. 173.

Ben Solomon, A. (2016). Jihadist Groups Using Facebook, Twitter to Spread Their Mesage. The Jerusalem Post. Extraído el 14 de abril de 2016 de: http://www.jpost.com/Middle-East/Jihadist-groups-using-Facebook Twitter-to-spread their-message-363050

Caracuel Raya, M. A. (2002). La OTAN ante la cumbre de Praga. Real Instituto Elcano. ARI Nº 104, p. 2

Caro Bejarano, M. J. (2010). Alcance y ámbito de la seguridad nacional en el ciberespacio. Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio.. Cuadernos de Estrategia. Instituto Español de Estudios Estratégicos, nº 149., p. 78

Casciani, D. (2015). Islamic State web accounts to be blocked by new police team, BBC News, Junio 2015. Extraído el 14 de abril de 2016 de: http://www.bbc.com/news/world-europe-33220037

Chimbelu, Ch. (2015). Social network intensify efforts to crackdown on jihadists. DW. Extraído el 19 de abril de 2016: http://www.dw.de/social-networks-intensify-efforts-to-crackdown-on-jihadists/a-18318205

Conway, M. (2007). Terrorism and Internet governance: core issues. Disarmament Forum. Vol. 3, pp 27-31.

Enríquez González, C. (2012). Estrategias internacionales para el ciberespacio. Ministerio de Defensa: Instituto Español de Estudios Estratégicos. Extraído el 13 de noviembre de 2015 de: http://dialnet.unirioja.es/servlet/oaiart?codigo=4540379

Eunjung C., A. (2005). Watchdogs seek out the web´s bad side. Washington Post. Extraído el 9 de abril de 2016 de: www.washingtongpost.com/wpdyn/contetn/article/2005/04/24/AR2005042401473.html

Gellman B., Timberg C. & Rich S. (2013). Secret NSA documents show campaign against Tor encrypted network. The Washington Post.4 de Octubre de 2013. Extraído el 23 de abril de: https://www.washingtonpost.com/world/national-security/secret-nsa-documents-show-campaign-against-tor-encrypted-network/2013/10/04/610f08b6-2d05-11e3-8ade- 1f23cda135e_story.html

Hannigan, R. (2014). The Web is a Terrorist's Command and Control Network of Choice. Extraído el 13 de noviembre de 2015 de: http://www.ft.com/cms/s/2/c89b6c58-6342-11e4-8a63-00144feabdc0.html#axzz3eBXGu0zh.

Lejarza, E. (2015). Terrorismo Islamista en las Redes-La Yihad Electrónica. Documento de Opinión. Instituto Español de Estudios Estratégicos 2015, nº 100, p. 18.

Narrillos, E. (2016). El Parlamento aprueba la directiva sobre registro de datos de pasajeros (PNR). En Portada. Extraído el 14 de abril de 2016 de: http://www.europarl.europa.eu/news/es/news-room/20160407IPR21775/El-Parlamento-aprueba-la-directiva-sobre-registro-de-datos-de-pasajeros-%28PNR%29.

Stalinsky, Steven y Sosnow. (2015). Encryption Technology Embraced By ISIS, AlQaeda, Other Jihadis Reaches New Level With Increased Dependence On Apps, Software –Kik, Surespot, Telegram, Wickr, Detekt, TOR Parte IV. Extraído el 08 de abril de 2016 de: http://cjlab.memri.org/latest-reports/encryption-technology-embraced-by-isis-al-qaeda-other-jihadis-reaches-new-level-with-increased-dependence-on-apps-software-kik-surespot-telegram-wickr-detekt-tor-part-iv-f/.

Weinmann, G. (2014). New Terrorism and New Media. Wilson Center Research Series. Vol. 2. Extraído el 13 de noviembre de 2015 de: https://www.wilsoncenter.org/publication/new-terrorism-and-new-media

PUBLICACIONES OFICIALES

ASOCIACIÓN INTERNACIONAL DE ABOGADOS, DIVISIÓN PRÁCTICA FORENSE. Report of theTask Force on Extraterritorial Jurisdiction. 2008.

COMISIÓN EUROPEA. GRUPO DE EXPERTOS EN MATERIA DE RADICALIZACIÓN VIOLENTA: Radicalisation processes leading to acts of terrorism 2008.

EC-COUNCIL PRESS. Computer Forensics: Investigating Data and Image Files. Nueva York: 2010

EUROJUST: Foreign Fighters: Eurojust´s View son the Phenomenom and the Criminal Justice Response. Updated Report. Enero 2015

EUROPOL. Comunicado de la Oficina de Europea de Policía. 3 de enero de 2011. Extraído el 8 de enero de 2016 de: www.europol.europa.eu/content/press/cybercrime-presents-major-challenge-law-enforcement-523.

FISCALÍA GENERAL DEL ESTADO. Memoria de la Fiscalía General del Estado 2015. Madrid: 2015.

GOBIERNO DE ESPAÑA. Estrategia de Ciberseguridad Nacional. Madrid: 2013

GOBIERNO DE ESPAÑA. Estrategia de Seguridad Nacional. Un proyecto compartido. Madrid: 2013.

GRUPO DE ESTUDIOS EN SEGURIDAD INTERNACIONAL. La reforma de los delitos de terrorismo mediante la Ley Orgánica 2/2015. Granada: 2015.

MINISTERIO DE INTERIOR. Estrategia Integral Contra el Terrorismo Internacional y la Radicalización (EICTIR). Madrid: 2012.

MINISTERIO DE INTERIOR. Plan Estratégico Nacional de Lucha contra la Radicaliza-

ción Violenta (PEN-LCRV). Madrid: 2015.

MINISTERIO DE LA PRESIDENCIA. Acuerdo para afianzar la unidad en defensa de las libertades y en la lucha contra el terrorismo. Madrid: 2015.

OFICINA DE LAS NACIONES UNIDAS CONTRA LA DROGA Y EL DELITO. Compendio de casos relativos a la lucha contra el terrorismo. 2010.

OFICINA DE LAS NACIONES UNIDAS CONTRA LA DROGA Y EL DELITO. El uso de Internet con fines terroristas. Viena: 2013.

OFICINA DE LAS NACIONES UNIDAS CONTRA LA DROGA Y EL DELITO Manual de buenas prácticas para incautarse de pruebas electrónicas. UNODOC. Viena: 2013.

OFICINA DE LAS NACIONES UNIDAS CONTRA LA DROGA Y EL DELITO. Preguntas frecuentes sobre cuestiones de derecho internacional de la lucha contra el terrorismo. Viena: 2009.

OFICINA DEL ALTO COMISIONADO DE LAS NACIONES UNIDAS PARA LOS DERECHOS HUMANOS. Los derechos humanos, el terrorismo y la lucha contra el terrorismo. Septiembre 2008

OFICINA DE PROGRAMAS JUDICIALES. Investigations Involving the Internet and Computer Networs. Instituto Nacional de Justicia. Departamento de Justicia de Estados Unidos: 2007.

Fecha de recepción: 18/11/2016. Fecha de aceptación: 20/12/2016