REVISTA
TRIBUNA INTERNACIONAL

VOL. 9 NÚM. 18 (2020) • PÁGS. 59-79 • DOI 10.5354/0719-2584.2020.58699
RECIBIDO: 28/9/2020 • APROBADO: 4/12/2020 • PUBLICADO: 31/12/2020

ARTÍCULOS

# Ciberseguridad y terrorismo

*Cybersecurity and terrorism*

**Ludmila Denise Ponce**
*Universidad Austral, Argentina*

**Mariano Rabaia** **Gonzalo Astuni**
**y Francisco Brocca**
*Universidad de Buenos Aires, Argentina*

**Matías Gasave**
*Pontificia Universidad Católica Argentina*

**RESUMEN** El surgimiento de Internet trajo consigo un sinfín de aplicaciones a nuestra vida cotidiana, con nuevas posibilidades y desafíos. El mundo criminal no ha sido ajeno a esta aparición, obteniendo provecho de la anonimidad que la *web* conlleva. En el siguiente trabajo, se centrará el foco en el uso de la red y la tecnología por parte de los grupos terroristas a través de tres marcos principales: teórico, jurídico y fáctico. Para ello, se precisarán definiciones de *ciber* y *terrorismo*, para luego aproximarse al concepto *ciberterrorismo*. Se trae a colación normativa relativa al tema en cuestión y finalmente se mencionan recientes casos de ciberterrorismo.

**PALABRAS CLAVE** Terrorismo, ciberterrorismo, ciberseguridad, infraestructura crítica.

**ABSTRACT** The emergence of the Internet has brought an endless application field within our everyday lives, with new possibilities and challenges. The criminal world has not been external to such appearance, taking advantage of the anonymity given by the world wide web. Internet and technology usage by terrorist groups will be the focal point of this paper, through three main frameworks: theoretical, legal and factual. *Cyber* and *terrorism* definitions will be specified in order to round the concept *cyberterrorism*. Legislation upon the subject will be presented, as well as recent cases of cyberterrorism.

**KEYWORDS** Terrorism, cyberterrorism, cybersecurity, critical infrastructure.

## Introducción

En el presente artículo se tratará de describir y definir el rol emergente que la tecnología ocupa en la concreción de actos terroristas, en un intento de proporcionar una definición clara, precisa y útil de lo que se entiende por *ciberterrorismo*.

Con los profundos cambios que han ocurrido con el surgimiento de Internet —y, consecuentemente, con la aparición de las redes sociales y el almacenamiento masivo de información digital—, la tecnología ha llegado para transformar el mundo de forma radical. Actualmente es parte esencial de la vida de muchas personas y ha traído aparejada muchas oportunidades y desafíos.

De acuerdo con la información recabada por el Banco Mundial, en el año 2017 aproximadamente el 50% de la población mundial usaba habitualmente internet[1]. Esta cifra no solo incluye a los usuarios corrientes, sino también a aquellos con fines malintencionados –estafadores, narcotraficantes, terroristas y demás criminales–. En este sentido, no es absurdo remarcar que, si bien la tecnología ha ganado terreno en todos los ámbitos de la vida y colabora con el desarrollo de las sociedades contemporáneas, también es un medio que utiliza la delincuencia, que no se quedará al margen de este proceso de digitalización.

La tecnología y el ciberespacio ofrecen beneficios inigualables a los criminales, tales como el anonimato, la posibilidad de llevar a cabo sus acciones de manera remota –ausencia de barreras geográficas y temporales– y los bajos costos de operación. En este aspecto, es oportuno mencionar que las investigaciones relacionadas con este tipo de actos delictivos han demostrado que la percepción moral de un criminal que actúa en el ciberespacio es distinta a la de un criminal que opera en el mundo físico. Los estudios socio-psicológicos indican que producto de la situación de amparo que les brinda la imposibilidad de ser identificados, junto con la minimización de los riesgos derivados de la confrontación física y la interacción remota con las consecuencias de sus actos, los criminales del ciberespacio se sienten vigorizados y muestran menos remordimiento y sentido de responsabilidad ante su accionar. Todo ello, aumenta las posibilidades de que se cometan delitos en el ciberespacio con mayor frecuencia (Murray y otros, 2019: 8).

De este modo, el presente trabajo se centrará en el tratamiento del terrorismo cibernético y el uso que los grupos terroristas hacen de las nuevas tecnologías; se precisarán los conceptos de *ciber* y *terrorismo* por separado, luego se arrojará una posible definición de *ciberterrorismo* y se lo diferenciará de otras clases de ciberagresiones. Por último, se hará mención de la normativa y de algunos casos acontecidos en el mundo que podrían llegar a encuadrar en la categoría de actos de ciberterrorismo

1. Para más información consultar el sitio web del Banco Mundial: http://bit.ly/38QJCex.

(ya que, como veremos más adelante, esta etiqueta dependerá de la definición de ciberterrorismo que se adopte).

Este trabajo pretende exponer la existencia de un peligro intrínseco de la sociedad moderna y permanentemente interconectada en la que vivimos, y resaltar la necesidad de actuar de manera anticipada a partir de medidas conducentes que permitan prevenir la materialización de actos de ciberterrorismo, evitando daños irreversibles.

## Prefijo ciber

De acuerdo con el *Diccionario de la Real Academia Española*, el prefijo *ciber-* (a partir del cual se forman conceptos cotidianamente utilizados como ciberespacio, cibernauta, ciberataque, entre otros) deviene de la castellanización del término inglés *cyber* que, a su vez, es el acortamiento de la palabra *cybernetic*. Luego, en la lengua española, se traduce como *cibernética*, término que define la ciencia que estudia las analogías entre los sistemas de control y comunicación de los seres vivos y de las máquinas y, en lo que aquí importa, aquello perteneciente o relativo a la realidad virtual, creado y regulado mediante una computadora. En este orden de ideas, el diccionario de marras señala que este prefijo indica relación con redes informáticas.

En consecuencia, se entenderá que este afijo representa una relación con los medios electrónicos de comunicación, particularmente, internet.

## Concepto de terrorismo

Observando el contexto mundial actual, existe una notoria y creciente preocupación por el terrorismo; la lucha contra aquel ha pasado a ocupar un rol central en la agenda política internacional de los últimos años. Ello explica, por ejemplo, la creación del Comité contra el Terrorismo dentro de la estructura de Naciones Unidas en el año 2017 y la creciente voluntad de los Estados de controlar la problemática a través de nuevas estructuras especializadas.

El secretario general de la Organización de las Naciones Unidas (ONU), Antonio de Oliveira Guterres, considera que la lucha contra el terrorismo y la prevención contra la violencia extrema es una de las más altas prioridades de las Naciones Unidas, ya que representa una creciente amenaza a la paz y seguridad internacionales. En este sentido, la preocupación resulta evidente al estudiar las estadísticas que revelan que, desde 1970 hasta la fecha, han acontecido más de 170.000 actos terroristas alrededor de todo el mundo (según la Base de Datos Mundial de Terrorismo) (Murray y otros, 2019: 10). El aumento de la destructividad y frecuencia de las acciones terroristas deben servir como un estímulo eficaz para avanzar en la elaboración de normas y criterios generales que contribuyan a proteger a la comunidad internacional de esta amenaza.

No obstante, el problemático debate sobre qué se entiende por terrorismo no ha arrojado certezas sobre su definición. En este sentido, las opiniones divergentes sobre la materia no han confluido en un consenso sobre las particularidades de este delito y, transitivamente, tampoco han podido definir inequívocamente sus motivos, técnicas, recursos y objetivos. A su vez, estas indefiniciones han obstaculizado la tipificación del terrorismo y la elaboración de estrategias políticas que permitan domar este fenómeno e, incluso, han repercutido en el abordaje de una convención de carácter universal que regule la materia: aún no se ha alcanzado una voluntad unánime de los Estados para lograr un tratado de prevención y sanción del delito de terrorismo.

Ahora bien, nos encontramos frente a un aspecto sobre el que no hay discusión: la capacidad de la comunidad internacional para afrontarlo está directamente ligada con el progreso que se alcance en la unificación de criterios en la definición, tipificación y contextualización del terrorismo. Este es el único camino hacia la consagración de normas que permitan su prevención y respuesta ante ataques. Patricia Kreibohm sostiene que «la definición, caracterización e interpretación que se haga de dicho fenómeno, condicionará los medios y los fines que se desarrollen para prevenirlo, contenerlo o combatirlo» (Kreibohm, 2002: 1-2).

Lamentablemente, las consideraciones de la autora continúan vigentes en la actualidad, dado que el *statu quo* no ha sido modificado:

> Hasta la fecha, el Sistema Internacional no ha logrado establecer la obligatoriedad del cumplimiento de normas para la prevención y la represión del terrorismo, lo cual ha derivado en que cada Estado tome sus propias decisiones al respecto y actúe individualmente en función de sus intereses y de sus posiciones ideológicas. En este marco de situación, las respuestas contraterroristas han adquirido un carácter heterogéneo y confuso, lo cual ha dificultado aún más la concentración de los esfuerzos y la adopción de criterios comunes que faciliten el diseño de políticas coordinadas, adecuadas y eficaces (Kreibohm, 2002: 1-2).

Como ya mencionamos, no existe actualmente una definición unánime —o, al menos, una que cuente con un amplio consenso universal—. Un estudio español afirma que existen más de 120 definiciones de terrorismo.[2] Incluso, diversos expertos en la materia sostienen que el término *terrorismo* ha sido manipulado para desacreditar a rivales políticos y enemigos, en lugar de brindar una definición objetiva sobre la problemática. Dentro de las numerosas definiciones que existen, una de las más recientes ha sido la formulada e incluida en el informe final del 2004 por el Grupo de

2. Rafael Calduch Cervera, «La problemática conceptualización jurídica del Terrorismo Internacional», conferencia pronunciada en la Universidad de Castilla-La Mancha, Cuenca, noviembre de 2001. Obtenido de Kreibohm (2002: 3).

Expertos de Alto Nivel sobre las amenazas, los desafíos y los cambios, nombrado por el secretario general de Naciones Unidas, que lo define como:

> Cualquier acto, además de los ya especificados en los convenios y convenciones vigentes sobre determinados aspectos del terrorismo, los convenios de Ginebra y la Resolución 1566 del Consejo de Seguridad de Naciones Unidas (2004), destinado a causar la muerte o lesiones corporales graves a un civil o a un no combatiente cuando el propósito de dicho acto, por su naturaleza o contexto, sea intimidar a una población u obligar a un Gobierno o a una organización internacional a realizar una acción o abstenerse de hacerla (ONU, 2004: 54).

En el ámbito académico, si bien tampoco existe unanimidad, se ha logrado cierto entendimiento en lo que se ha descrito como un «consenso académico» —un acuerdo entre los especialistas—, que según la formulación de Alex Schmid y Albert Jongman se puede expresar de la siguiente manera:

> El terrorismo es un método productor de ansiedad basado en la acción violenta repetida por parte de un individuo o grupo (semi) clandestino o por agentes del Estado, por motivos idiosincráticos, criminales o políticos, en los que —a diferencia del asesinato— los blancos directos de la violencia no son los blancos principales. Las víctimas humanas inmediatas de la violencia son generalmente elegidas al azar (blancos de oportunidad) de una población blanco, y son usadas como generadoras de un mensaje. Los procesos de comunicación basados en la amenaza —y en la violencia— entre el terrorista (la organización terrorista), las víctimas puestas en peligro y los blancos principales son usados para manipular a las audiencias blanco, convirtiéndolas en blanco de terror, blanco de demandas o blanco de atención, según que se busque primariamente su intimidación, su coerción o la propaganda (Schmid y Jongman, 1988: 28; la traducción es nuestra).

Matías Álvarez Dorrego, por su parte, ha identificado cuatro elementos característicos de los actos y actividades terroristas:

> 1. poseen como objetivo próximo la dominación de algo/alguien, rechazar y subvertir el orden jurídico e internacional vigente, forzar a determinados individuos, grupos, comunidades y/o Estados a efectuar concesiones a favor de los objetivos terroristas;
> 2. provocan la alteración de la paz pública, mediante la amenaza o el empleo de la violencia con resultados catastróficos;
> 3. crean un clima de inseguridad, turbación y terror colectivo a corto plazo o en forma inmediata en virtud del carácter clandestino e imprevisible del ataque;
> 4. generan un riesgo injusto padecido por la comunidad social, siendo esta una víctima inocente (Álvarez Dorrego, 2004: 95-96).

Como podemos observar, todas las teorías confluyen en la idea de que el terrorismo consiste en el uso ilegal de la fuerza o la violencia con el objeto de intimidar o coaccionar, a través del terror, a otros actores para que tomen medidas que impliquen cambios políticos, sociales o económicos. En palabras del asesor de la Europol y catedrático, Manuel R. Torres Soriano, «el terrorismo siempre implica el uso de la violencia o una amenaza creíble del empleo de esta».[3]

## Marco teórico: Ciberterrorismo

Concluida esta breve introducción, corresponde adentrarse en el tema que atañe al presente trabajo. La tipificación del ciberterrorismo como una forma específica de terrorismo resulta adecuada y necesaria, dado que requiere actores, herramientas y respuestas preventivas y correctivas distintas al terrorismo convencional.

El término ciberterrorismo se estableció en 1980 por Barry Collin, bajo la percepción de una convergencia entre los dos mundos, el virtual y el físico. (Pérez Gómez, 2020: 3). Posteriormente, Mark M. Pollitt precisó concretamente el fenómeno al definirlo como «ataque predeterminado, políticamente motivado, contra información, sistemas y programas informáticos y datos a través de la red, como acto violento contra objetivos no combatientes por organizaciones o agentes clandestinos» (Pollitt, 1998: 9).

Sin embargo, es preciso indicar que, de la misma forma que ocurre con el término descrito precedentemente, «ciberterrorismo» no cuenta con una definición unánimemente aceptada por la comunidad internacional. Sin embargo, se pueden distinguir dos grandes corrientes en relación a su definición: por un lado, una «pura» o restrictiva y, por otro lado, una más amplia.

Los primeros sostienen que «ciberterrorismo» es todo ataque terrorista cuyo objetivo es dañar una infraestructura crítica. Se entiende por infraestructura crítica aquellos elementos y sistemas propiedad de un Estado, que son, según Torres Soriano, «esenciales para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, el bienestar social y económico de la población, y cuya perturbación o destrucción afectaría gravemente a un Estado».[4]

Dentro de esta vertiente se encuentra la definición elaborada por la investigadora en seguridad de la información, Dorothy E. Denning, que dispone que ciberterrorismo es todo ataque ilegal y amenaza de ataque contra computadoras, redes informáticas y la información en ellas almacenada, realizados para intimidar o coaccionar a un Gobierno o su gente con un fin político o social. Asimismo, agrega que dicho

3. Manuel R. Torres Soriano, entrevista en el *El País*, 14 de octubre de 2018, disponible en https://bit.ly/2L9jYJN.

4. Manuel R. Torres Soriano, véase nota anterior.

ataque deberá causar un daño contra la propiedad o las personas o al menos tener la magnitud suficiente como para generar miedo (Denning, 2000).

En esta línea, también encontramos la definición de Dan Verton, retomada por Sánchez Medero:

> El ciberterrorismo es la ejecución de un ataque sorpresa por parte de un grupo terrorista extranjero subnacional con objetivo político utilizando tecnología informática e Internet para paralizar o desactivar las infraestructuras electrónicas y físicas de una nación, provocando de este modo la pérdida de servicios críticos, como energía eléctrica, sistemas de emergencia telefónica, servicio telefónico, sistemas bancarios, Internet y otros muchos (Sánchez Medero, 2015: 101).

La segunda vertiente, más amplia que la anterior, sostiene en definirlo como todo ataque en el cual los sistemas de computación o Internet juegan un rol preponderante en la configuración del acto terrorista, independientemente de que el objetivo sea o no un sistema de computación (Murray y otros, 2019: 14). En este grupo, encontramos la definición propuesta por Jeffrey F. Addicott, quien precisa que el ciberterrorismo es «el empleo de varios recursos de computación para intimidar o coaccionar a otro para alcanzar objetivos específicos» (Sánchez Medero, 2015: 101).

En suma, el debate consecuente se centra en torno a aceptar que el ciberterrorismo se limita exclusivamente a ataques contra infraestructuras críticas, o si, contrariamente, permite incluir aquellos actos en los que las computadoras ocupan un rol sustancial como medio o herramienta para llevar a cabo el hecho terrorista.

En lo que respecta a la definición empleada en este capítulo, se propone considerar al ciberterrorismo como cualquier amenaza o ataque conducido contra o a través de medios electrónicos de computación por parte de actores—predominantemente no estatales— con el fin de intimidar o coaccionar a un Gobierno en miras de conseguir un determinado objetivo político, ideológico o social. La definición aquí empleada incluye toda acción en la cual el componente cibernético juega un rol preponderante y esencial, con independencia de si se atacan funciones o información computarizada de importancia crítica, u otros objetivos no informáticos. Paralelamente, y de forma similar al terrorismo convencional, el ciberterrorismo busca generar daños físicos o psicológicos, pero primordialmente buscará que esos efectos se desplieguen sobre una amplia audiencia.

Por último, para definir un acto ciberterrorista, es necesario determinar el grado de participación de los componentes cibernéticos en la configuración del acto en concreto: los componentes cibernéticos y tecnológicos empleados para llevar a cabo el ataque deben haber ocupado una función principal y fundamental, de manera tal que el acto existe principalmente gracias a su naturaleza cibernética. Asimismo, el agente que lleva a cabo el acto debe contar con habilidades y un grado de *expertise* considerablemente superior al del usuario promedio de cibertecnologías.

En procura de arrojar mayor claridad sobre el concepto en cuestión, es preciso distinguir y diferenciar esta forma de ataque con otras formas de agresión conducidas también por medios cibernéticos —léase ciberacoso, cibercrimen, hacktivismo, ciberespionaje y guerras cibernéticas— y entender la entidad e independencia de cada figura.

## Otras formas de ciberagresión

Ciberacoso: es también denominado acoso virtual y definido como el uso de medios cibernéticos —como redes sociales— para acosar, molestar a una persona o grupo de ellas, a través de mensajes con connotación negativa o divulgación de información confidencial o falsa. Si bien tiene diferentes formas de perpetrarse (*cyberbullying, sextorsion*, ciberviolencia de género o *grooming*), no es habitual que esté tipificado y solo en algunos ordenamientos puede constituir un delito.

Cibercrimen: según la definición elaborada por el Consejo de Europa en el Convenio de Budapest, es «toda acción dirigida contra la confidencialidad, integridad o disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos».[5] Puede identificarse como los casos de *hacking* o *cracking*, que consisten en el acceso no autorizado a un sistema de computación con el fin de robar información personal de la víctima almacenada en dicho sistema o para introducir *malware* y utilizarlo para extorsionar.

Esta figura delictiva encuentra su correlato en el mundo físico en los llamados crímenes convencionales, como el fraude, el robo de identidad y el narcotráfico que, en principio, no utilizan medios cibernéticos, pero que pueden ser facilitados y potenciados si son cometidos a través de computadoras. La nota distintiva es el objetivo de quien lleva a cabo un cibercrimen: obtener una ganancia económica u otro fin de índole personal, pero no político o social.

Hacktivismo: implica una combinación entre activismo y el uso de las herramientas de *hacking* para protestar en Internet; es decir, el uso ilegal o legal de herramientas digitales para fines políticos y de protesta. En palabras de Vicente «no se interpreta como una acción criminal, sino como una forma legítima de protesta que se concentra en objetivos gubernamentales o empresariales para incitar un boicot, la desobediencia civil digital o convocar un mitin ciberespacial. Activismo puro, vía Internet, donde la red es usada como un agente para la justicia social de base a través de varias acciones de protesta» (Vicente, 2004: 2).

Espionaje cibernético: las metodologías y herramientas del espionaje han ido evolucionando conforme el avance de las tecnologías y, en los tiempos actuales, ante la

5. Consejo de Europa, «Convención sobre la Ciberdelincuencia», Budapest, 23 de noviembre de 2001, disponible en https://bit.ly/34Umrik.

vasta tecnología y su disponibilidad, el espionaje no solo se ha complejizado, sino que ha aumentado considerablemente.

Siendo ello así, y teniendo en cuenta que el espionaje consiste en el acto de obtener acceso no autorizado a información sensible con el fin de conocer las capacidades y aspiraciones de otro sujeto, el espionaje cibernético —específicamente— tiene lugar cuando aquel acto es desarrollado a través de sistemas de computación y medios electrónicos. En este punto, lo sensible y perjudicial de este delito es que puede ser conducido de manera remota y permite robar una cantidad de información ilimitada. Consecuentemente, podría causar daños de magnitud incalculable.

Guerra cibernética: son todos aquellos actos de guerra llevados a cabo en el ciberespacio, que pueden asociarse con tecnologías de la información y cuyos agentes son Estados nacionales u organizaciones internacionales que tienen como objetivo dañar los sistemas de computación e información y la infraestructura crítica de otro Estado u organización internacional, a fin de compeler al enemigo. La clave de esta figura se encuentra en el sujeto que lleva a cabo las acciones: debe tratarse de un Estado.

Teniendo en cuenta lo expuesto hasta aquí, es pertinente concluir que el ciberterrorismo tiene entidad delictiva propia, requiere de acciones, objetivos y móviles específicos para su tipificación y solo comparte los medios utilizados —cibernéticos— con los delitos arriba enunciados.

## Uso de internet por grupos terroristas: Estado actual del ciberterrorismo

Los investigadores sostienen que los terroristas utilizan la *web* para diferentes propósitos. Como ya mencionamos, los criminales en general han encontrado grandes beneficios a la hora de actuar en el ciberespacio: no solo los ampara el anonimato, sino que también disponen de grandes caudales de información accesible, una comunicación fácil y eficaz y bajos costos económicos (Çelisksoy y Ouma, 2019: 244).

En esta misma línea, Sánchez Madero ha señalado:

> Prácticamente, todos los grupos delictivos disponen de algún tipo de espacio (*web*, foro, *site*, etc.) en la red. Bien sea para divulgar la historia de la organización y sus actividades, la información sobre sus objetivos políticos e ideológicos, las críticas de sus enemigos, o simplemente, para verter amenazas o abrir foros de debate e interactuar con sus seguidores y simpatizantes. Aunque eso sí, no siempre son fáciles de encontrar ni de acceder, ya que como cabe suponer suelen ser perseguidos por los servicios policiales y de inteligencia de los distintos Gobiernos. De ahí que por norma general, se mantengan poco tiempo en una misma dirección, cambiando constantemente de ubicación, o que su acceso se encuentre limitado por un administrador (Sánchez Medero, 2015: 101).

En este aspecto, la Internet es utilizada por los terroristas para una amplia gama

de actividades relacionadas con sus propósitos, tales como la diseminación de propaganda, la radicalización, influencia y reclutamiento de individuos, el acceso a información sensible de los Estados y las sociedades, el entrenamiento virtual de sus miembros, la financiación de sus actividades y la planificación y concreción de ataques (Macdonald y Mair, 2015: 15). De esta forma, el uso de la red por estos grupos extremistas es una preocupación que abarca mucho más que la específica figura del ciberterrorismo: tanto el ataque, como todas las medidas preparatorias y previas a éste, son llevadas a cabo en el plano virtual. Siendo ello así, es posible identificar diferentes actividades que se relacionan con el delito de ciberterrorismo. A saber:

Diseminación de propaganda: el medio virtual se utiliza como difusor de la propaganda para legitimar las operaciones terroristas y para ganar apoyo o demostrar las debilidades de sus enemigos. En este orden de ideas, la divulgación de sus actos es fundamental para sus objetivos, constituyendo una de las prioridades. Los grupos terroristas han encontrado en Internet un medio de difusión de su propaganda con beneficios inigualables; a diferencia de los medios de comunicación tradicionales (radio, televisión, periódicos), les permite llegar sin restricciones, sin filtros y con costos ínfimos a un gran número de personas (Weimann, 2004: 7). En el año 2010 ya había alrededor de 10.000 sitios web para la difusión de material violento y terrorista. Es un desafío distinguir entre las actividades prohibidas, como la propaganda terrorista, y la legítima defensa de un punto de vista (Diputados de la República Argentina, 2019: 2).

Radicalización y reclutamiento de individuos: las redes cibernéticas son una herramienta ideal para los grupos terroristas, dado que permiten el contacto y la comunicación con individuos vulnerables y aquellos que tienen algún tipo de interés e inclinación hacia los ideales terroristas, pudiendo adoctrinarlos en sus creencias y religión (Janbek y Williams, 2014: 299).

Es sabido que los terroristas utilizan toda la gama de alternativas que ofrece la *web* (redes sociales, salas de chat, foros, etcétera) a fin de captar nuevos adeptos e iniciar el proceso de radicalización —que se ha acelerado vertiginosamente por la supresión de las barreras espaciales y temporales—. En este punto es pertinente mencionar el caso de los llamados «lobos solitarios», que son definidos como terroristas que llevan a cabo sus ataques de manera independiente del grupo al cual adhieren (Spaaij, 2010: 854). En palabras de Chamorro, «el Estado Islámico parece estar priorizando la captación de jóvenes europeos con conocimientos y formación en nuevas tecnologías con el objetivo de crear su propio «ciberejército»».[6]

Entrenamiento en línea y planificación de ataques: los grupos terroristas utilizan ampliamente Internet como herramienta de capacitación y entrenamiento de sus

6. Enrique F. Chamorro, «El Estado Islámico y la ciberguerra», *Real Instituto Elcano*, 20 de mayo de 2015, disponible en https://bit.ly/300jcxx.

miembros. De hecho, los investigadores sostienen que el ciberespacio es la «universidad *online* de los terroristas» (Weimann, 2006: 15).

En este sentido, diferentes pesquisas desarrolladas por los Departamentos de Defensa de varios Estados han determinado que existen espacios y plataformas dedicados exclusivamente al entrenamiento y capacitación de terroristas, en los cuales los miembros pueden interactuar realizando preguntas y compartiendo conocimientos y experiencias; incluso, pueden acceder a una amplia bibliografía que engloba manuales, enciclopedias, artículos y videos instructivos. Con el uso de las herramientas digitales, los grupos extremistas pueden capacitar e instruir a sus miembros de forma remota y segura, sin la necesidad de trasladarlos. Como ejemplo de ello tenemos la revista *Inspire*, propiedad de Al Qaeda, con el objetivo declarado de permitir a los musulmanes entrenarse para la *yihad* en su casa (Oficina contra la Droga y el Delito de las Naciones Unidas, 2012: 3).

Por otra parte, el ciberespacio también resulta una herramienta eficaz a la hora de planear la logística de un embate, además de ser imprescindible para la adquisición de elementos necesarios en la ejecución de atentados. Los atacantes no solo necesitan de una comunicación fluida entre quien lo ejecuta y quien lo idea, sino también requieren de ciertos trabajos preparatorios que incluyen la identificación y el estudio del objetivo de ataque, el reconocimiento del sitio donde se desarrollará, la selección de rutas y alternativas de escape, la investigación de los momentos de mayor congestión de individuos y la efectividad y tiempos de respuesta de los servicios de emergencia. Este tipo de tareas demandan de múltiples visitas y estudios al lugar de ataque que conllevarían altos riesgos y costos para los terroristas. En este sentido, la *web* les ha permitido sortear todos esos obstáculos (Macdonald y Mair, 2015: 21).

Financiamiento en línea: los medios cibernéticos brindan una plataforma donde los grupos terroristas pueden obtener financiamiento fácil, barato y expedito para el sostenimiento de sus actividades. También garantiza el anonimato del donante y los receptores.

En esta línea, las Naciones Unidas han identificado cuatro formas en que los terroristas usan Internet para obtener financiamiento; a saber: solicitud directa, *e-commerce*, uso de herramientas de pago en línea y triangulación mediante organizaciones caritativas (Oficina contra la Droga y el Delito de las Naciones Unidas, 2012: 7). A éstas, podemos sumarle el vertiginoso avance y rol de las criptomonedas, que son merecedoras de un capítulo aparte.

Como ocurre con el lavado de activos, el financiamiento del terrorismo es de difícil prevención, detección, identificación e investigación, en tanto requiere de elevados conocimientos técnicos y herramientas sofisticadas con las que muchos países no cuentan —en especial, los menos desarrollados—. Por ello, resulta de suma importancia lograr la cooperación de la comunidad internacional en esta materia.

Puede afirmarse que, actualmente, el ciberespacio —y la tecnología en general— constituye una herramienta indispensable para los grupos terroristas, poniendo énfasis en la necesidad de diseminar su propaganda para esparcir exponencialmente sus propuestas. Asimismo, les permite reclutar y radicalizar nuevos miembros a través de su entrenamiento y capacitación en línea y planificar y preparar nuevos ataques.

En este punto, si bien diversos expertos sostienen que los grupos extremistas aún no cuentan con el nivel suficiente de sofisticación para atentar contra la infraestructura crítica de un Estado —dado que se encuentran aún en una etapa de desarrollo prematuro del ciberterrorismo—, son los Estados quienes deben activar la búsqueda urgente de medidas mancomunadas para prevenir los ataques de este estilo, y otras tendientes a paliar las posibles consecuencias que conllevaría un ataque de esta índole.

## Marco jurídico: legislación

En este apartado, trataremos de analizar cuáles son las medidas legislativas tomadas en diferentes jurisdicciones para abordar la problemática expuesta.

Al igual que ocurre con el término *terrorismo*, desarrollado anteriormente, la falta de consenso universal en torno a la definición de ciberterrorismo conlleva una cuasi inexistente legislación en la materia.

Sin perjuicio de esto, en muchos países se encuentran tipificados una gran cantidad de delitos informáticos y se imponen gravosas sanciones para los ataques a los sistemas públicos protegidos.[7]

En el plano multilateral, a pesar de que las Naciones Unidas han establecido una Estrategia Global contra el Terrorismo (Res. A/RES/60/288), una Guía sobre Buenas Prácticas para la Protección de Infraestructuras Críticas Contra Ataques Terroristas (2018) y, en diciembre del mismo año, han puesto en funcionamiento el Pacto Mundial de Coordinación de la Lucha Antiterrorista de las Naciones Unidas, continúa siendo competencia de cada Estado el juzgamiento y condena de los actos terroristas en base a su legislación.

El Consejo de Seguridad de la ONU ha dictado varias resoluciones en el marco del capítulo VI de la Carta de las Naciones Unidas. Éstas conllevan una especial importancia para entender la gravedad del delito analizado y la necesidad de activar los

7. En Argentina, se encuentra promulgada desde el día 24 de junio del año 2008 la Ley 26.388 que regula la materia. También encontramos los artículos 153 bis y 157 del Código Penal. Brasil: Ley 12.737. Chile: Ley 19.233. Bolivia: artículo 363 del Código Penal. Colombia: Artículo 269A, C de la Ley de Protección de la Información y de los Datos. Ecuador: Artículo 59, Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Ley No. 2002-67). Perú: Artículo 207-A del Código Penal. Venezuela: Gaceta Oficial 37.313. Oct/2010. Ley Especial sobre delitos informáticos.

procesos de normativización en el plano internacional. En la Resolución S/RES/2370, el Consejo ha expresado su preocupación por «el creciente uso, en una sociedad globalizada, de las nuevas tecnologías de la información y las comunicaciones, en particular internet, por los terroristas y quienes los apoyan para facilitar la comisión de actos terroristas, así como su uso con fines de incitación o reclutamiento, o para financiar o planificar actos terroristas».

Asimismo, en la Resolución A/RES/72/284 se ha alentado «a los Estados Miembros a que trabajen de consuno para garantizar que los terroristas no encuentren cobijo en línea, al tiempo que promueven un Internet abierto, interoperable, fiable y seguro que promueva la eficiencia, la innovación, la comunicación y la prosperidad económica, respetando el derecho internacional, incluido el derecho de los derechos humanos».

En el ámbito de la Organización de Estados Americanos (OEA), el Comité Interamericano contra el Terrorismo (CICTE) se encuentra constantemente trabajando con los Estados partes para reforzar las medidas de seguridad informática. En lo que aquí interesa, en el Informe Anual de 2017, en su sección de Fomento de la Capacidad de Lucha contra el Terrorismo, se dejó asentado que «por medio del «Programa Integral de Fortalecimiento de la Seguridad Cibernética de las Américas», y con el apoyo financiero de los Gobiernos de los Estados Unidos, Canadá, España, Estonia e Inglaterra, así como del sector privado, el CICTE ha contribuido a fortalecer las capacidades de los Estados Miembros para detectar amenazas cibernéticas y prevenir, responder y recuperarse de incidentes cibernéticos». Asimismo, se encuentra trabajando con los diferentes miembros de la Organización para elaborar distintas estrategias nacionales de ciberseguridad, reforzar las capacidades de detección temprana de ciberintrusiones, formar un espacio para compartir información, capacitar a los ciudadanos en cuestiones de seguridad digital y desarrollar reportes estatales sobre ciberseguridad.

En esta inteligencia, el mentado Comité también dictó la Resolución CICTE 1/18, por la cual se acordaron medidas de fomento de la confianza regional para promover la cooperación en el ciberespacio de acuerdo a las directrices elaboradas por el Grupo de Expertos Gubernamentales de las Naciones Unidas. A tal fin, en el seno de la organización, se creó el Grupo de Trabajo sobre Medidas de Fomento de Cooperación y Confianza en el Ciberespacio que, con carácter permanente, busca elaborar y discutir nuevas medidas para fortalecer la seguridad cibernética regional.

Por otra parte, la cumbre del G20 reunida en Osaka (Japón) en 2019 convocó a las plataformas en línea a unirse en la lucha contra el ciberterrorismo y el extremismo violento que conduce al terrorismo. Así, por medio de una declaración conjunta, se insta a prohibir el uso de plataformas con fines delictivos y crear términos y condicio-

nes para detectarlos y prevenirlos. Este desafío exige la rápida adaptación de los sistemas de defensa y el desarrollo de competencias específicas en esta esfera particular.[8]

Creemos que es de suma importancia y necesidad que, en el corto plazo, los Estados activen sus procesos de creación de normas en su plano interno y, al mismo tiempo, negocien una regulación marco a nivel internacional. Hoy en día es prudente tener en miras que gran parte de la vida de los seres humanos ocurre en el mundo cibernético, donde constantemente se están ingresando datos. De acuerdo con las recomendaciones del Centro de las Naciones Unidas para la Lucha contra el Terrorismo, la cooperación entre los Estados es un área en la que la protección de la soberanía, los derechos de los ciudadanos y el patrimonio nacional debe ser armonizado con el necesario intercambio de información y recursos para prevenir y luchar contra posibles actos de terrorismo y violencia extrema en el ciberespacio (Diputados de la República Argentina, 2019: 3). Asimismo, resulta imperiosa la adopción de legislación que regule la educación y concientización del público general, la cooperación con el sector privado para resguardar las infraestructuras críticas, la regulación de los estándares mínimos que debe cumplir cualquier producto que pueda llegar a tener impacto en estas infraestructuras, y la responsabilidad de los proveedores de servicios de Internet.

Sin embargo, la regulación de esta materia no resulta sencilla debido a que la actividad terrorista evoluciona y se adapta a las medidas de seguridad que los Estados van aplicando; es decir, es un peligro dinámico y cambiante. Además, debemos de tener en cuenta que los avances tecnológicos son muy rápidos —a las antípodas del derecho—: en la carrera por la tipificación de conductas como penalmente atribuibles, los Estados van detrás y la tarea de legislar se dificulta.

En esta inteligencia, existen diversas razones que atentan contra la prevención y persecución del ciberterrorismo. Por un lado, la ausencia de una convención de Naciones Unidas contra el terrorismo internacional —como se ha señalado anteriormente—y de consensos mínimos en el seno de la comunidad internacional en relación a este crimen dificulta la tarea de normar y tomar medidas mancomunadas en materia de ciberterrorismo. Por otro lado, gran parte de la doctrina opina que todavía no ocurrió un suceso que haya podido ser identificado como *ciberterrorismo*, cuestión que también dificulta el asentamiento de una definición unívoca de este fenómeno; como bien sabemos, el derecho sucede a los hechos. Consecuentemente, la cooperación internacional se ve obstruida. La combinación de los factores descriptos genera que los instrumentos de derecho internacional se encuentren plagados de términos vagos, ambiguos y abstractos, delegándose así en los Estados la obligación de perseguir y penar este crimen (Pérez Gómez, 2020: 3).

8. G20, «Statement on Preventing Exploitation of the Internet for Terrorism and Violent Extremism Conducive to Terrorism», Osaka, 29 de junio de 2019, disponible en https://bit.ly/38G6qxE.

## Marco fáctico: casos

Asentado el marco teórico y jurídico, es oportuno mencionar algunos casos que, a modo de ejemplo, pueden, dependiendo de la definición por la cual se opte (estricta o amplia), representar actos de ciberterrorismo. En este sentido, como se ha mencionado, gran parte de la doctrina prefiere opinar que aún no se han cometido ataques que puedan encuadrarse dentro del delito analizado; las nociones de ciberagresión y ciberterrorismo tienen límites poco claros y pueden confundirse en la práctica. Sin perjuicio de ello, es pertinente remarcar algunos hechos aislados que, *a priori*, podrían representar actos de esta categoría.

Siendo ello así, lo ocurrido en Estonia, en el año 2007, podría encuadrar —por lo menos de forma generalizada— en la definición. Sucintamente, ese año el Estado decidió trasladar la estatua del Soldado de Bronce del centro de la capital —Tallin— a un cementerio en la periferia; ese monumento había sido puesto por los rusos cuando derrotaron a la Alemania nazi en la Segunda Guerra Mundial. Por un lado, ese gesto fue visto como una victoria para quienes son parte de la etnia estonia, pues consideraban que el ejército soviético invadió y oprimió a su pueblo durante 50 años hasta la disolución de la URSS. Por otro lado, los estonios de origen ruso lo vieron como una ofensa, dado que, para ellos, la estatua representaba la victoria soviética sobre el régimen de Hitler. Esto ocasionó diversas revueltas y movilizaciones que terminaron con un muerto, varios heridos y más de un millar de detenidos. Inmediatamente, el Gobierno de Rusia se plegó a la queja social.

Consecutivamente, un ataque a gran escala vulneró las ciberdefensas estonias y destruyó las estructuras informáticas de los poderes públicos, telecomunicaciones, sitios periodísticos, entidades financieras y partidos políticos. En este sentido, si bien diversos medios periodísticos han afirmado que el ataque tuvo su origen en el seno del Gobierno ruso, desde la administración del Estado estonio han sostenido que las pruebas no son concluyentes.[9]

En síntesis, en lo que atañe a este hecho, el sesgo político del ataque, la escala masiva de aquel y la vulneración de una red informática permite encuadrar —con prudencia— este acto dentro de la noción de ciberterrorismo brindada.

En otro punto —y a modo de ejemplificar las medidas tomadas por los Estados respecto de las acciones que tienen lugar en el ciberespacio y cuyas características las hacen objeto de este trabajo—, es preciso aludir a la orden de arresto emitida por el Departamento de Justicia de Estados Unidos contra un grupo de nueve ciudadanos

9. Damien McGuinness, «Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país», *BBC*, 6 de mayo de2017, disponible en http://bbc.in/3mXVWPi, y Ricardo Martínez de Rituerto, «Los «ciberataques» a Estonia desde Rusia desatan la alarma en la OTAN y la UE», *El País*, 17 de mayo de 2018, disponible en https://bit.ly/38LY1Ja.

iraníes con fecha 23 de marzo de 2018. Los acusados ejercían como líderes, contratistas, asociados, *hackers* a sueldo o afiliados al Instituto Mabna, una compañía de origen iraní que, desde al menos el año 2013, coordinó una campaña de ciberintrusiones en sistemas computarizados; entre los afectados se pueden encontrar 144 universidades estadounidenses, 176 universidades de otros países, 47 compañías del sector privado, tanto dentro como fuera del territorio estadounidense, el Departamento de Trabajo de Estados Unidos, la Comisión Federal Reguladora de Energía, los Estados de Hawái e Indiana, las Naciones Unidas y Unicef.

A través de las actividades de los imputados, el Instituto Mabna logró sustraer más de 31 *terabytes* de información académica y propiedad intelectual de universidades, además de cuentas de correo electrónico de empleados de compañías del sector privado, agencias gubernamentales y organizaciones no gubernamentales. Las diversas acciones, sostiene el comunicado, fueron cometidas en nombre de los Cuerpos de la Guardia Revolucionaria de Irán. Pese a ello, el Gobierno iraní no ha emitido comentarios al respecto.

Por su parte, el fiscal federal Geoffrey S. Berman resaltó que los procesados tienen ahora el estatus de fugitivos de la justicia estadounidense y que «solamente podrán ver el mundo (fuera de Irán) a través de sus pantallas, pero habiendo perdido su activo más importante: anonimidad».[10]

Otro caso que podría ser asociado al ciberterrorismo es el ataque cibernético dirigido contra el Bundestag alemán en 2015 con el objetivo de robar información sensible. Al respecto, la canciller alemana, Angela Merkel, aseguró que existían pruebas contundentes de que el Gobierno ruso estaba detrás del ataque y que se trataba de una estrategia de guerra híbrida.

En cuanto al hecho, se llevó a cabo a través de un correo electrónico dirigido al parlamento que, aparentemente, provenía de las Naciones Unidas con información sobre el conflicto en Ucrania. Este iba acompañado de un virus que comenzó a diseminarse sobre todo el sistema de información del órgano legislativo germano, que se paralizó. Mientras el Gobierno alemán intentaba restablecer las defensas, los atacantes, a través de este *malware*, pudieron absorber toda la información disponible.

Luego de una investigación de 5 años, la canciller aseguró que detrás del ataque estaba el Departamento Central de Inteligencia ruso (GRU) y solicitó a la Unión Europea sanciones contra el jefe de inteligencia militar rusa. Para ello, promovió la activación de un nuevo mecanismo llamado «Conjunto de Instrumentos de Ciberdiplomacia» que se creó para imponer sanciones a personas involucradas en ciberataques. Estas medidas impulsadas en el seno de la Unión Europea sirven para responder,

10. Traducción propia de fragmento de Comunicado de prensa de la U.S. Attorney's Office, Southern District of New York, Department of Justice de Estados Unidos, 23 de marzo de 2018, disponible en http://bit.ly/38SyQo3.

disuadir o impedir actividades cibernéticas malintencionadas contra la Unión o sus Estados miembros.[11]

Por su parte, recientemente, en mayo de 2020, se produjo un ataque cibernético en el servidor israelí *uPress*, que es utilizado por miles de usuarios. En este sentido, a través de este sitio se reprodujo un video que mostraba diversos ataques aéreos y explosiones en la ciudad de Tel Aviv y al primer ministro, Benjamín Netanyahu, tratando de huir de la ciudad en llamas. Además, el video contenía un mensaje en inglés y en hebreo que decía «prepárense para una gran sorpresa»; luego, agregaba que «la cuenta regresiva para la destrucción de Israel comenzó hace mucho tiempo» y, en el final, aparecía la frase «Israel no sobrevivirá los próximos 25 años». Por último, se intentó obtener acceso a las cámaras *web* de los usuarios a través de un enlace.

Si bien no existen pruebas concluyentes sobre la autoría del ataque, los medios de comunicación lo atribuyeron al grupo Hackers of Saviour. Otra de las hipótesis que tomó relevancia es la que atribuye el ataque a la República Islámica de Irán, en tanto el video presenta diversas banderas y símbolos del país persa; incluso, días después, un ataque cibernético en el puerto iraní de Shahid Rajaee fue atribuido a Israel. Por último, la hipótesis con mayor sustento y respaldo por parte de los especialistas en seguridad y por el Gobierno israelí sostiene que se trataría de *hackers* iraníes ubicados en Turquía, Gaza y el norte de África.[12]

Este ejemplo quizás sea el más preciso para definir ciberterrorismo —vinculado a la definición propuesta—, en tanto se trata de un grupo no estatal que lleva a cabo un ataque desde y hacia medios electrónicos de computación y tiene una clara intención de intimidar y coaccionar con un fin político.

Finalmente, desde el enfoque de la prevención, cabe referirse a lo sucedido en los Países Bajos. Allí, la ministra de Defensa, en la conferencia de prensa del 4 de octubre de 2018, afirmó que sus servicios de inteligencia habían logrado desbaratar un ciberataque ruso contra la Organización para la Prohibición de las Armas Químicas (OPAQ), con sede en La Haya. El director de la agencia de inteligencia militar holandés mostró, en su presentación, la antena, computadoras personales y otro equipamiento que los espías pretendían utilizar para violar la seguridad de la red de wifi de la OPAQ; en ese momento, la organización se encontraba comprobando la identidad de la sustancia utilizada en el ataque al exespía ruso Sergei Skripal y su hija, realizado en Salisbury, Inglaterra, en marzo de 2018. Los cuatro ciudadanos rusos fueron capturados en abril y deportados a Rusia.[13]

---

11. Ana Carbajosa, «Merkel acusa a Rusia del «escandaloso» ciberataque al Bundestag en 2015», *El País*,13 de mayo de 2020, disponible en https://bit.ly/3pzSb4o.

12. «Hackearon cientos de Israel y dejaron un video amenazante: «Prepárense para una sopresa»», *Infobae*, 21 de mayo de 2020, disponible en https://bit.ly/3nZfqEy

13. Anthony Deutsch y Stephanie van den Berg, «Dutch government says it disrupted Russian at-

Tanto la Unión Europea como la OTAN, han repudiado las acciones ordenadas por el Kremlin, sosteniendo que «socavan la legislación y las instituciones internacionales» (OTAN: 2018).[14] Por su parte, el Ministerio de Asuntos Exteriores ruso tildó de absurdas las acusaciones.[15]

En este apartado, es posible visualizar que, a pesar de las dificultades que se han mencionado en los párrafos previos, los Estados se encuentran implementando medidas, tanto preventivas como punitivas, a fin de limitar—y en algún momento erradicar— las maniobras delictivas ciberterroristas.

## Conclusiones

Finalmente, corresponde esbozar una serie de conclusiones en torno a las problemáticas proyectadas a lo largo de todo este capítulo.

En el plano teórico, es posible identificar, cuanto mínimo, dos problemas sustanciales que dificultan la comprensión del delito. En primer lugar, el mayor debate que se presenta en la actualidad es la incapacidad de encontrar una definición unánime —o al menos mayoritaria— tanto para el concepto de terrorismo como para el de ciberterrorismo. En segundo lugar —y vinculado con el primero—, la imposibilidad de calificar de forma precisa los diferentes delitos que se perpetran en el escenario cibernético a fin de individualizarlos y delimitarlos con claridad; los límites son difusos y ello dificulta la tarea preventiva y punitiva. La consecuencia de estos inconvenientes se refleja a la hora de legislar, lo cual se evidencia en normas repletas de términos vagos y ambiguos que dificultan su efectiva aplicación.

En tal sentido, uno de los mayores desafíos que enfrentan los Estados es la necesidad de desarrollar e invertir en tecnologías y capacitaciones técnicas para que sus agentes puedan combatir de forma adecuada este tipo de delitos. Por otro lado, las diferencias sociales y económicas entre los diferentes Estados y el consecuente desequilibrio tecnológico generan que muchos Estados que se encuentran reforzados y fuertes en materia de ciberseguridad sean vulnerados indirectamente a través de ataques a países cuyas defensas virtuales sean bajas o fáciles de derribar.

Debido a su carácter transversal, este fenómeno demanda una cooperación entre los sectores públicos, privados y la propia sociedad, al encontrarse en juego los derechos humanos, la defensa, la economía y el desarrollo tecnológico. Esta cooperación

---

tempt to hack chemical weapons watchdog», *Reuters*, 4 de octubre de 2018, disponible en http://reut.rs/34YnIVO.

14. Traducción propia de un fragmento de comunicado de la OTAN, «Statement by NATO Secretary General Jens Stoltenberg on Russian cyber attack», 4 de octubre de 2018, disponible en: https://bit.ly/34TKzlr.

15. Andrew Osborn, «Russia calls Dutch chemical weapons watchdog hacking claims absurd: RIA», *Reuters*, 4 de octubre de 2018, disponible en http://bit.ly/38IKqlC.

multisectorial constituye una de las mejores herramientas para acelerar la respuesta contra los ciberataques, aumentando el intercambio de información y coordinando esfuerzos conjuntos. De esta forma se logrará mejorar la legislación, la tecnología, la innovación, y el intercambio de información y datos para lograr una eficaz lucha contra el ciberterrorismo (Diputados de la República Argentina, 2019: 3).

Para poder conseguir una buena estrategia de seguridad es necesario un plan integral que vaya evolucionando y se vaya adaptando a este tipo de amenaza, que lleva la iniciativa y que se multiplica como consecuencia del atractivo de su alto nivel de impunidad (Pérez Gómez, 2020: 3).

Finalmente, no debe perderse de vista que la tecnología —y, consecuentemente, el ciberespacio— son instrumentos fundamentales para el desarrollo de las sociedades. El *quid* de la cuestión pasará entonces por la forma en la que los Estados y sus estructuras logren efectivamente proteger a los individuos y garantizarles la libertad de acceso y navegación por el ciberespacio, sin cruzar la delgada línea de restringir o censurar el derecho a la información y privacidad. Como sostiene Torres Soriano:

> Si [los terroristas] consiguen degradar la vida en sociedad hasta el punto de una renuncia expresa a su parcela de libertad para librarse de una amenaza, ellos habrán logrado su objetivo de empeorar nuestras vidas. Renunciar a parte de la privacidad debe ser el último recurso, si se han agotado todas las alternativas. Son procesos difíciles de revertir. Cuando uno formaliza la pérdida de privacidad, no se recupera automáticamente cuando la amenaza ha sido neutralizada.[16]

## Referencias

Álvarez Dorrego, Matías (2004). *La Corte Penal Internacional. Hacia la inclusión en el Estatuto de Roma del Crimen de Terrorismo*. Buenos Aires: Fabián J. Di Plácido editor.

Çelisksoy, Ergül y Smith Ouma (2019). «Terrorist Use of the Internet». *Bilişim Hukuku Dergisi*, Social Sciences University of Ankara. Disponible en https://bit.ly/34ULotZ.

Denning, Dorothy E. (2000). «Statement». Georgetown University. Disponible en https://bit.ly/34J3NtB.

Janbek, Dana y Valerie Williams (2014). «The role of the Internet Post-9/11 in Terrorism and Counterterrorism». *Brown Journal of World Affairs*, 20 (2).

Kreibohm, Patricia (2002). Ponencia «El terrorismo internacional: ¿Guerra o Delito? La polémica en torno a la interpretación de un fenómeno inquietante», Univer-

16. Manuel R. Torres Soriano, entrevista brindada al *Diario El País*, 14 de octubre de 2018, disponible en https://bit.ly/2L9jYJN.

sidad Nacional de La Plata, Instituto de Relaciones Internacionales, Primer Congreso en Relaciones Internacionales del IRI. Disponible en https://bit.ly/38DzhT6.

Macdonald, Stuart y David Mair (2015). «Terrorism Online: A new strategic environment». En Lee Jarvis, Stuart MacDonald y Thomas Chen (editores), *Terrorism Online: Politics, Law and Technology*. Abingdon: Routledge (1).

Murray, Gregg R.; Craig Douglas Albert; Kim Davies; Candace Griffith; John J. Heslen; Lance Y. Hunter; Nadia Jilani-Hyler y Sudha Ratan (2019). «Towards creating a new research tool: Operationally defining cyberterrorism», Augusta University. Disponible en https://bit.ly/3mUCwLj.

ONU, Organización de las Naciones Unidas (2000). «Delitos relacionados con redes informáticas. Documento de antecedentes para el curso práctico sobre delitos relacionados con las redes informáticas», Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente, (A/CONF.187/10). Disponible en https://bit.ly/2Mig5D8.

—. (2004) Informe del Grupo de alto nivel sobre las amenazas, los desafíos y el cambio, «Un mundo más seguro: la responsabilidad que compartimos», (A/59/565). Disponible en https://bit.ly/3aPCUIw.

—. (2019a) «Carta de fecha 21 de febrero de 2019 dirigida a la Presidencia del Consejo de Seguridad por el Grupo de Expertos establecido en virtud de la resolución 1874 (2009)», (S/2019/171). Disponible en https://bit.ly/3hwoaPZ.

—. (2019b) Informe del secretario general de las Naciones Unidas sobre la «Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos». Disponible en https://bit.ly/3pzPYpv.

Pérez Gómez, Amanda (2020). «Ciberterrorismo, ¿una nueva amenaza?», Documento de opinión IEEE 106/2020. Disponible en https://bit.ly/34TxJDM.

Pollitt, Mark M. (1998). «Cyberterrorism: Fact or Fancy». *Computer Fraud & Security*, 1998 (2). Disponible en https://bit.ly/2JutLKf.

Sánchez Medero, Gema (2015). «El ciberterrorismo: de la web 2.0 al Internet Profundo». *Revista Ábaco, 2da época*, 3 (85). Disponible en https://bit.ly/37YoXqo.

Schmid, Alex P. y Albert J. Jongman (1988). *Political Terrorism: A new guide to Actors, Authors, Concepts, Data Bases, Theories and Literature*. Nueva Jersey: Transaction Publishers.

Spaaij, Ramón (2010). «The Enigma of Lone Wolf Terrorism: An Assessment», *Studies in Conflicts & Terrorism*, 33 (9). Disponible en https://bit.ly/37VvsK4.

Vicente, Loreto (2004). «¿Movimientos sociales en la Red? Los hacktivistas». *El Cotidiano*, 20 (126). Disponible en https://bit.ly/3hyF4O3.

Weimann, Gabriel (2004). «www.terror.net, How Modern Terrorism Uses the Internet», United States Institute of Peace, Special Report N° 116. Disponible en https://bit.ly/38HWDY1.

—. (2006). «Terror on the Internet: the new arena, the new challenges», United States Institute of Peace. Disponible en https://bit.ly/3hvhwdo.

## Reconocimiento

El presente trabajo se desarrolló en el marco del Proyecto IUS «El Terrorismo internacional. Desafíos actuales del derecho penal local e internacional» (2019-2021) de la Pontificia Universidad Católica Argentina, dirigido por la Dra. Sofía J. Danessa.

## Sobre los autores

Ludmila Denise Ponce es abogada (UCA). Becaria en Derecho Público e Instituciones de la Unión Europea (Universidad de Alicante, España). Investigadora del Observatorio de Ciberdelincuencia y Evidencia Digital de la Universidad Austral (Argentina). Su correo electrónico es ludmila.deniseponce@cpacf.org.ar.

Mariano Rabaia es abogado de la Universidad de Buenos Aires. Ayudante docente de la materia Derecho Internacional Público (Facultad de Derecho, UBA). Prosecretario Coadyuvante -int- del Juzgado Contencioso Administrativo y Tributario N° 1 de la Ciudad Autónoma de Buenos Aires. Su correo electrónico es marianorabaia@derecho.uba.ar. https://orcid.org/0000-0001-9319-3996.

Gonzalo Astuni es abogado de la Universidad de Buenos Aires. Ayudante docente de las materias Fuentes del Derecho Internacional y Sujetos y Jurisdicciones (Facultad de Derecho, UBA). Consultor jurídico en la Comisión Cascos Blancos del Ministerio de Relaciones Exteriores, Comercio Internacional y Culto de la República Argentina. Su correo electrónico es gastuni@derecho.uba.ar. https://orcid.org/0000-0002-2577-0787.

Francisco Brocca es abogado de la Universidad de Buenos Aires. Ayudante docente de la materia Derecho Internacional Público (Facultad de Derecho, UBA). Oficial 2° del Juzgado de Responsabilidad Penal Juvenil núm. 2 de San Martín, Provincia de Buenos Aires.

Matías Gasave es estudiante de Relaciones Internacionales (UCA). Buenos Aires, Argentina. Su correo electrónico es matias.gasave@gmail.com.

## REVISTA TRIBUNA INTERNACIONAL

La *Revista Tribuna Internacional* busca fomentar la reflexión, el debate, el análisis y la comunicación pluralista y con rigor científico en las áreas del derecho internacional público, derecho internacional privado, relaciones internacionales y derecho internacional de los derechos humanos. Los artículos y ensayos son seleccionados mediante revisión de pares externos a la Facultad de Derecho de la Universidad de Chile. Se reciben trabajos en castellano y en inglés.


EDITOR GENERAL

Luis Valentín Ferrada Walker

SITIO WEB

tribunainternacional.uchile.cl

CORREO ELECTRÓNICO

revistatribuna@derecho.uchile.cl





La edición de textos, el diseño editorial
y la conversión a formatos electrónicos de este artículo
estuvieron a cargo de Tipográfica
(www.tipografica.io)