RESPUESTA INTERNACIONAL AL DESAFÍO DE LA ESTRATEGIA MEDIÁTICA DEL ESTADO ISLÁMICO

INTERNATIONAL RESPONSE TO THE CHALLENGE OF ISLAMIC STATE MEDIA STRATEGY

Alicia Chicharro Lázaro*

RESUMEN: Considerado internacionalmente como un grupo terrorista, el Estado Islámico (EI) ha proclamado su Califato que de momento se extiende por amplias zonas dentro de Irak y varias ciudades sirias, pero que aspira a asentarse en el conjunto de territorios alguna vez sometidos a la influencia musulmana. El éxito de su ofensiva se debe en gran medida a su poderío militar, pero también a una cuidada estrategia en los ámbitos económico, social y mediático. Respecto a este último, el EI está realizando una agresiva campaña de propaganda, a través de diversos medios de difusión y fundamentalmente utilizando las redes sociales. Gracias a ello ha logrado que ciudades enteras se rindan a sus pies, que grupos de personas se desplacen buscando refugio ante la amenaza de su llegada y que musulmanes radicales de occidente se interesen por la organización, se conviertan en simpatizantes o incluso se unan a sus filas. En el presente trabajo trataremos de analizar la problemática jurídica de las actividades ciberterroristas del EI, enmarcándolas en la lucha internacional contra el terrorismo de alcance global y teniendo en cuenta la protección de derechos fundamentales como la libertad de expresión y el acceso a la información.

ABSTRACT: Considered as a terrorist group from an international point of view, the Islamic State (ISIS) has proclaimed a Caliphate. This new territorial entity occupies for the moment wide areas of Iraq and some Syrian towns, but it aims to establish itself in all the territories sometime under Islam. To a large extent the success of its offensive is due not only to its military force, but also to a careful propaganda strategy, carried out through different media and essentially through the social networks. Thanks to this, the ISIS has achieved the surrender of entire towns, the displacement of peoples seeking refuge prior to its advance, and the interest of extreme Western Muslims towards the organization, turning them into supporters or even combatants. This paper aims to analyze the legal aspects of the ISIS cyberterrorism within the fight against global terrorism, taking into account the protection of human rights as the freedom of speech and the right to information.

PALABRAS CLAVE: Ciberterrorismo, Estado Islámico, terrorismo yihadista, UNESCO

KEYWORDS: Cyberterrorism, Islamic State, jihadi terrorism, UNESCO

Fecha de recepción del original: 30 de enero de 2015. Fecha de aceptación de la versión final: 4 de mayo de 2015

* Profesora Contratada Doctora de Derecho Internacional Público de la Universidad Pública de Navarra. Correo electrónico: alicia.chicharro@unavarra.es

 DOI: 10.17103/reei.29.07

I. INTRODUCCIÓN

En los últimos meses, el denominado Estado Islámico (EI o ISIS, si utilizamos su acrónimo en inglés)[1] se ha hecho un hueco casi permanente en las secciones de noticias internacionales en todos los medios de comunicación. Este protagonismo se debe, por una parte, a sus victorias militares y, por otra, a una cuidada propaganda que circula como la pólvora por Internet.

Todas las voces coinciden en señalar que se trata de una nueva organización terrorista emparentada de alguna manera con Al Qaeda. A su calificación como terrorismo y a las consecuencias que la misma conlleva, han contribuido sobremanera los distintos documentos gráficos que circulan por la red donde se muestran atrocidades como decapitaciones o ejecuciones en masa. A su vez, el propio EI publica informes cuantificando las distintas acciones desarrolladas (atentados con coche bomba, atentados suicidas, etc.), algunas de ellas características del terrorismo si consideramos la función política que persiguen.

Sin embargo, ellos no se definen como organización terrorista sino que se denominan "Estado", término sin duda deliberado ya que los Estados poseen el monopolio del uso legítimo de la violencia. Además, su estrategia propagandística intenta emular la comunicación institucional de un Estado.

El hecho de ser un Estado o una comunidad beligerante no le inmuniza ante la adjetivación de terrorista. No olvidemos que el terrorismo como concepto político distintivo recibe su nombre (y buena parte de su mala fama) de las acciones llevadas a cabo por quienes ostentaban el poder político estatal[2]. Y además se trata de terrorismo internacional, pues su dimensión transfronteriza, al menos en sentido jurídico, radica en que sus acciones perturban las relaciones internacionales y la comunidad internacional en su conjunto las considera contrarias a las normas deseables de conducta.

La complejidad de esta organización yihadista que controla un determinado territorio por el que despliega fuerzas armadas comparables con las de cualquier ente estatal, pero que además amenaza con expandirse, supone un enorme desafío para la comunidad internacional. La respuesta unilateral por parte de determinados Estados, solos o en pequeñas coaliciones, no debería ser la estrategia a seguir. Consideramos que la ONU, como organización garante de la paz y seguridad internacionales, está llamada a dar los

[1] También se suelen utilizar las siglas en español EIIL (Estado Islámico de Irak y el Levante) o en inglés ISIL (Islamic State of Iraq and the Levant) o simplemente IS (Islamic State). Su acrónimo en árabe es DAESH (al-Dawla al-Islamiya al-Iraq al-Sham). Parece que las autoridades de los países de la UE habrían llegado a un acuerdo informal para utilizar esta última denominación, aunque ese pacto ha tenido muy poco seguimiento por parte de los medios de comunicación.

[2] La Convención Francesa del año II de la Revolución Francesa, 1793-94, declaró la *patrie en danger* y utilizó el terror para proteger la Revolución de sus enemigos. Bien es verdad que al aludir al Estado se suele hablar de "terror" porque este término hace referencia a la consecuencia de una seria violencia represiva, mientras "terrorismo" sería la demostración de violencia deliberadamente planeada; TOWNSHEND, C., *Terrorismo*, Alianza, Madrid, 2002, p. 90. Sin embargo, ni esta fútil distinción ni el escaso tratamiento científico del terrorismo de Estado, nos deben llevar a negar su existencia.

DOI: 10.17103/reei.29.07

pasos necesarios para que la intervención armada contra el EI obtenga el adecuado respaldo jurídico-internacional.

Pero, ¿qué hacemos contra su propaganda en Internet? La respuesta no es fácil, ya que las soluciones drásticas como prohibir el acceso a Internet o cerrar la válvula de oxígeno publicitario que le dan las redes sociales, no están resultando efectivas dada la propia arquitectura del ciberespacio. A su vez la persecución, enjuiciamiento y sanción de estas conductas en unos Estados mientras en otros siguen impunes, trasluce un escenario internacional descoordinado que solo favorece a los terroristas.

II. EVOLUCIÓN DEL ESTADO ISLÁMICO

El EI es parte del movimiento "yihad global". Este movimiento no es un todo coherente y organizado, sino que más bien se caracteriza por compartir una ideología, el salafismo yihadista, una versión fundamentalista y belicosa del Islam suní basada en un estado de guerra religiosa permanente contra los regímenes apóstatas del mundo árabe y sus aliados extranjeros[3].

En el terreno político, su primer anhelo apunta a la restauración del viejo sistema de gobierno denominado Califato. Este imperio político panislámico abarcaría el conjunto de los territorios en los que rigen o han regido alguna vez, desde el siglo VII, los preceptos del Corán.

Los antecedentes de esta organización yihadista se remontan a 2006, cuando surge con el nombre de Estado Islámico de Irak[4]. Después de algunas victorias en territorio sirio amplió su apelativo pasando a llamarse Estado Islámico de Irak y Al-Sham (el Levante). El 29 de junio de 2014, se proclamó la restauración del Califato, a cuya cabeza se sitúa el que fuera líder de dicha organización y hoy Califa, Abu Bakr al-Baghdadi[5].

El antecedente remoto del actual EI se sitúa en el más amplio movimiento yihadista que se produjo en tierras árabes tras la invasión de Irak por parte de Estados Unidos en 2003. El que fuera el número dos de Al Qaeda, al-Zarqawi había conformado un grupo denominado Jam'at al-Tawhid wa-l-Jihad (Grupo de la Unidad y la Yihad) que centró sus esfuerzos no solo en expulsar a los invasores extranjeros, sino también en aterrorizar a la mayoritaria población chií de Irak. Este grupo prestó lealtad a Al Qaeda, aunque

[3] Véase ROSINY, S., "Der jihad. Historische und zeitgenössische Formen islamisch legitimierter Gewalt", in WERKNER, I-J. / LIEDHEGENER, A. (Hrsg.), *Gerechter Krieg gerechter Frieden. Religionen und friedensethische Legitimationen in aktuellen militärischen Konflikten*, VS Verlag für Sozialwissenschaften, Wiesbaden, 2009, pp. 225-244.

[4] Como se explicará más adelante, desde 2004 el grupo se encontraba integrado en Al Qaeda (Al Qaeda en Irak) y será en 2006 cuando se produzca la escisión de esa organización para convertirse en el actual EI.

[5] Parece que su nombre verdadero sería Ibrahim ibn Awwad al-Badri. Hasta el momento, su única aparición pública tuvo lugar el 4 de julio de 2014, cuando dio un sermón en la Gran Mezquita de Mosul. Véase ROSIGNY, S., "Des Kalifen neuner Kleider: Der Islamische Staat in Irak uns Syrien", *Institut für Nahost-Studien*, nº 6, 2014, p. 4, en http://www.giga-hamburg.de/en/system/files/publications/gf_nahost_1406.pdf (última consulta 25 noviembre 2014).

DOI: 10.17103/reei.29.07

dentro de esta organización se les criticó por sus métodos extremamente violentos, incluso se llegó a renombrar como Al Qaeda en Irak (AQI). Poco duro este grupo porque al-Zarqawi, junto a otros líderes de grupos yihadistas en Irak, estableció Majlis Shura al-Mujahidin (MSM)[6].

Con la muerte en 2006 de al-Zarqawi, aquel grupo se convirtió en el Estado Islámico, desde ese momento ya desligado de Al Qaeda[7]. Recientemente se ha llegado a afirmar que más que un aliado de Al Qaeda, el EI es un competidor[8]. Aunque ideológicamente ambas organizaciones pertenecen al salafismo yihadista y tienen en común su visión radical y agresiva del Islam, el EI adopta una concepción menos tolerante con lo que denominan sectas islámicas desviadas, particularmente con los chiíes[9].

Al Qaeda y el EI difieren particularmente en el plano organizacional. El EI ha dejado de ser una mera entidad yihadista para pasar a ser un Estado (dawla). La restauración del Califato también era una aspiración de Al Qaeda, pero nunca lo puso en práctica porque sus dirigentes insistían en que aún no se daban las condiciones favorables para crear y consolidar dicho proyecto[10].

Aunque Al Qaeda sea la organización más importante con la que compite el EI, no olvidemos que en la zona donde se asienta el nuevo Estado operan otros grupos y milicias[11]. Así mismo, el EI está consiguiendo implantarse en otras extensiones

[6] SALTMAN, E.M. and WINTER, C., *Islamic State: The Changing Face of Modern Jihadism*, Quilliam Foundation, London, 2014, p. 29.

[7] El actual líder de esta organización terrorista, Ayman al-Zawahiri ha puesto de relieve públicamente que su organización nunca fue consultada sobre la fundación del EI, la cual tuvo lugar tras una reunión de combatientes yihadíes en octubre de 2006. El propio EI corrobora esa afirmación en un documento oficial de dicha fecha cuando asegura lo siguiente: "This state of Islam has arisen anew to strike down its roots in the region, as was the religion's past one of strength and glory".

[8] BUNZEL, C., "Understanding the Islamic State (of Iraq and al-sham)", *Norwegian Peacebuilding Resource Centre, Expert Analysis*, July, 2014, p. 2, en http://www.peacebuilding.no (última consulta 10 septiembre 2014).

[9] El avance del EI por el territorio iraquí debe una gran parte de su éxito a una población suní harta de los abusos del anterior Primer Ministro al-Maliki. Esos mismos abusos han inducido la pasividad inicial de los peshmerga kurdos ante la amenaza del EI.

[10] Así, mientras el EI controla parte del territorio de Irak y Siria, Al Qaeda sigue siendo una organización clandestina cuya matriz sobrevive confinada en áreas montañosas de Afganistán y núcleos tribales de Pakistán. Véase WICHMANN, P., *Al-Qaida und der globale Djijad*, Springer, Heidelberg, 2014.

[11] En Irak, milicias suníes como Jamaat Ansar al-Sunnah, Jaish al-Mujahidin y Naqshabandiyya Way se han unido al EI. En Siria, además de otros grupos menos radicales, sigue operando Jabat al-Nusra (JN), considerada ahora una filial de Al Qaeda, aunque en realidad fue Abu Umar al-Baghdadi, primer líder del EI, quien encomendó a Abu Muhammad al-Jawlani la tarea de formar un frente para combatir contra el régimen alawita-chií del Presidente Bashar al-Assad. Entre 2011 y 2013 Jabat al Nusra y el EI no se han estorbado en posiciones sirias. Sin embargo, en abril de 2013, Abu Bakr al-Baghdadi, actual líder del EI, comenzó a sospechar que Jawlani quería zafarse de la tutela del EI, por lo que en una maniobra inesperada anunció la disolución de Jabat al-Nusra y la extensión del EI al territorio de la gran Siria, añadiendo a su nombre el término al-Sham. Jawlani se negó a disolver Jabat al-Nusra y juró lealtad al líder de Al Qaeda, al-Zawahiri. Inmediatamente, Al Qaeda exigió al EI que limitase sus actividades al territorio iraquí. Desobedeciendo esta orden, el EI se expandió por diversas ciudades sirias. Desde entonces entre ambas organizaciones se ha dado un clima de convivencia más que de enfrentamiento, con algunos episodios de transfuguismo.

DOI: 10.17103/reei.29.07

territoriales que antes eran feudo exclusivo de Al Qaeda[12]. Y, por último, los combatientes extranjeros procedentes del norte de África y de Europa se decantan por el EI, en vez de las otras milicias que operan en Siria y en Irak[13]. El nuevo Califato deslumbra a los musulmanes radicales residentes en países occidentales, algunos de los cuales estarían dispuestos a cometer atentados por su cuenta para contribuir a la causa[14]. Actualmente, el EI posee el control territorial de amplias zonas del norte de Siria y del noroeste de Irak, incluida la ciudad de Mosul, la segunda más grande del país[15].

Por un lado, no es casualidad que la primera implantación territorial se haya producido en Irak. Sabemos que la retirada de Estados Unidos, en diciembre de 2011, no dejó tras de sí ni un país pacificado ni mucho menos un Estado consolidado y eficiente. El yihadismo aprovechó esa coyuntura para convertir a Irak en el nuevo campo de batalla[16]. Precisamente la exitosa acometida del EI por el territorio iraquí se debe en gran medida a una población suní harta de los reiterados agravios del gobierno del anterior Primer Ministro (chií) Nuri al-Maliki[17].

Por otro lado, el avance del EI en Siria tiene su explicación en una guerra que se prolonga por más de tres años, que ha provocado millares de muertos y desplazados y que, sin embargo, no ha conseguido movilizar a la comunidad internacional para

[12] Sería el caso de Al Qaeda en la Península Arábiga (AQPA), Al Qaeda en el Magreb Islámico (AQMI) y otras entidades asociadas como Terik e Taliban Pakistán (TTP). Por otra parte, el EI ha recabado el apoyo de organizaciones yihadistas de reciente aparición como Ansar al Shari en Túnez y Libia, Jund al Jalifa en Argelia, Ansar Bayt al Maqdis en Egipto o Abu Sayaf en Filipinas. Incluso Boko Haram de Nigeria ha declarado su adhesion al EI.

[13] Véase SAID, B., *Islamischer Staat: IS-Miliz, al-Qaida und die deutschen Brigaden*, Beck, München, 2014. Existe incluso una célula de veteranos de Al Qaeda poco conocida hasta ahora denominada el grupo Jorasán que, según el Pentágono, preparaba un ataque "inminente" contra intereses occidentales como respuesta a los bombardeos aéreos de este país sobre posiciones del EI en Siria. La movilización de milicianos de Al Qaeda pone de manifiesto el respaldo de muchos de ellos a las acciones del EI, lo que desdibuja los límites entre las organizaciones yihadistas que operan en Oriente Medio.

[14] Es el caso de los denominados “lobos solitarios”, como algunos medios de comunicación calificaron a los hermanos Kouachi que atacaron la sede de la revista satírica Charlie Hebdo matando a 13 personas, o a Amedy Coulibaly que secuestró a varias personas en un supermercado judío de París, causando la muerte a cuatro rehenes y a dos policías en enero de 2015. Los primeros afirmaron pertenecer a Al Qaeda, versión corroborada por el máximo dirigente de la rama de esa organización en Yemen, mientras Coulibaly sería miembro del EI, aunque los tres estaban coordinados para llevar a cabo sus respectivas acciones terroristas. La investigación de los hechos determinará si se trataba de “lobos solitarios” o de células de las organizaciones yihadistas mencionadas. Véase SPAAIJ, R., *Understanding Lone Wolf Terrorism*, Springer, Heidelberg, 2012.

[15] COCKBURN, P., *ISIS. El retorno de la yihad*, Barcelona: Ariel, 2015, p. 13.

[16] NUÑEZ, J., “El delirio califal del Estado Islámico en Irak y Siria”, *Política Exterior*, sep-oct, 2014, p. 107.

[17] Recordemos que la minoría suní había disfrutado del poder desde la creación del Estado de Irak por los británicos en 1932. La invasión por parte de Estados Unidos en 2003 resultó en un liderazgo chií muy influido por Irán. El mandato del anterior Primer Ministro (chií) Nuri al-Maliki se caracterizó por su deriva autoritaria y la persecución de los adversarios políticos, llegando incluso a dictar órdenes de detención contra miembros de la plataforma electoral Al Iraqiyya, aliada gubernamental del Estado de la Ley liderado por el propio al-Maliki, y de destacados parlamentarios suníes. En un intento por equilibrar la situación, en agosto de 2014, se eligió como Primer Ministro al kurdo Haidar al-Abadi.

DOI: 10.17103/reei.29.07

ponerle freno[18]. Es más, el desamparo absoluto de los rebeldes sirios ha abierto la puerta a grupos yihadistas radicales, entre los que se ha hecho un hueco el EI. Las actividades del EI y del resto de organizaciones yihadistas se enmarcan dentro del terrorismo religioso de corte islamista.

Hoffman apunta las características centrales de este tipo de terrorismo: la primera, su función trascendental más que política, en el sentido de que se ejecuta como respuesta directa a una exigencia o imperativo teológico; la segunda, el hecho de que, al contrario que los seculares, los terroristas religiosos frecuentemente persiguen eliminar categorías de enemigos demasiado amplias y no se detienen ante los posibles efectos contraproducentes, en términos políticos, de una matanza indiscriminada; y finalmente, la particularidad más importante es que no intentan apelar a ningún otro grupo más que al suyo propio[19]. Matanzas indiscriminadas, objetivo que trasciende lo político, circunscripción a una particular comunidad, parece que no son características que encajen adecuadamente en otros tipos de terrorismo, como el revolucionario o el nacionalista. Sin embargo, no se trata de un fenómeno moderno[20], sino de una violencia acentuada en los últimos tiempos de manos de grupos yihadistas[21].

Como ya se ha señalado, ellos no se definen como organización terrorista sino como "Estado". Evidentemente, raro es el individuo o grupo que adopta para sí mismo el término terrorista; suelen ser los otros los que lo utilizan para referirse a ellos, fundamentalmente los gobiernos de los Estados que sufren su amenaza[22]. Al considerarse Estado, único actor que posee el monopolio del uso legítimo de la violencia dentro de sus fronteras, los yihadistas del EI pretenden desplegar todas las funciones y competencias estatales en los territorios conquistados, simulando así un orden en medio del caos.

A parte del poderío militar y del liderazgo ideológico, el EI posee sus propias fuentes de financiación que le han permitido no solo mantenerse todos estos años, sino también sufragar un desarrollado sistema administrativo estatal para los territorios controlados[23]. Se ha encargado de las labores de reconstrucción, reparando tendido eléctrico, arreglando carreteras, poniendo en marcha medios de transporte público, servicio de correos, asistencia social, etc.

[18] En relación con la guerra en Siria, véase KIRCHNER, M., "Vom syrischen Bürgerkrieg zum Flächenbrand?", in VERKNER, I-J. et als. (Hrsg.), *Friedengutachten 2014*, LIT Verlag, Münster, 2011, pp. 295-307.
[19] HOFFMAN, B., *Inside Terrorism*, Victor Gollancz, London, 1998, p. 85.
[20] Los zelotes, los asesinos y los thugs ya practicaron la violencia religiosa.
[21] JUERGENSMEYERS, M., *Terrorism in the Mind of God*, University of California Press, Berkley, 2000, p. 43. También RAPOPORT, D., "Why Does Religion Messianism Produce Terror?", in WILKINSON, P. (ed.), *Contemporary Research on Terrorism*, Aberdeen University Press, Aberdeen, 1987, p. 51 y ESPOSITO, J., *The Islamic Threat: Myth or Reality?*, Oxford University Press, New York, 1992, p. 135.
[22] TOWNSHEND, C., *Terrorismo*, Alianza, Madrid, 2002, p. 13.
[23] Véase RHEINBERG, B., "Islamischer Staat: Vom Terror zum Kalifat", *Blätter für deutsche und international Politik*, nº 9, 2014, p.50.

DOI: 10.17103/reei.29.07

Todo ello no sería posible sin una estrategia concreta con el objetivo principal de lograr la independencia financiera. La extorsión, los secuestros para cobrar rescates, el robo de bancos o la explotación de pozos de petróleo en los territorios bajo su control[24], son algunos de los medios para conseguir fondos para la organización, sin tener que depender de las donaciones individuales provenientes de países del Golfo Pérsico[25].

La actividad terrorista del EI tiene una función auxiliar o es una pieza más dentro de una estrategia militar más extensa. Se utiliza para ejercer una presión psicológica subjetiva facilitada, sobre todo, por el alarmismo colectivo[26]. Los terroristas buscan esa alteración sabiendo que si sus actividades no la producen, no llamarían la atención.

Precisamente, este objetivo se ha visto de sobra alcanzado con la campaña de propaganda mediática de sus actos terroristas a través de Internet, que utilizando de forma especial las redes sociales, ha logrado el alarmismo colectivo suficiente para despertar el interés de los medios de todo el mundo.

III. DIFUSIÓN DEL TERROR DEL ESTADO ISLÁMICO A TRAVÉS DE LAS TECNOLOGÍAS DE LA COMUNICACIÓN Y LA INFORMACIÓN

1. Los distintos usos de las TIC con fines terroristas

Internet y las nuevas tecnologías de la información pueden ser usados para propagar diversos contenidos terroristas: explicar sus razones o "justificaciones" de actos terroristas singulares, hacer propaganda y lanzar amenazas, encontrar nuevos adeptos y patrocinadores, y comunicarse regularmente con sus seguidores.

Hasta la era tecnológica los terroristas se tenían que conformar con una comunicación de escaso alcance sobre sus puntos de vista, objetivos y ambiciones, bien porque los métodos tradicionales de transmisión no llegaban a un gran público, bien porque tenían que preservar su anonimato. Por ejemplo, el empleo de panfletos para justificar sus acciones o el uso del boca a boca para el reclutamiento de nuevos miembros eran medios costosos en términos de tiempo y riesgo.

[24] El EI llegó a firmar un contrato de venta de energía con el gobierno de Bashar al-Assad, dándose la paradoja de que el dictador al que intentaban derrocar, de esta forma, les financiaba. Noticia aparecida en el *New York Times* de 29 de enero de 2014.

[25] Algunos analistas apuntan a las donaciones de Arabia Saudí que, sin duda, se deben al interés por financiar a grupos yihadistas suníes utilizados para revertir la ventaja alcanzada por Irán en su afán por convertirse en el líder regional. Véanse a este respecto NUÑEZ, J., "El delirio califal…", op. cit., p. 111; KAZIMI, N., "The Caliphate Attempted", *Hudson Institute's Current Trends in Islamist Ideology*, vol. VII, July, 2008, p. 37 y del mismo autor KAZIMI, N., "A Virulent Ideology in Mutation: Zarqawi Upstages Maqdisi", *Hudson Institute's Current Trends in Islamist Ideology*, vol. II, September, 2005, p. 60.

[26] Este alarmismo no equivale exclusivamente a miedo, la simple conmoción o excitación por la violencia puede provocar un impacto suficiente.

DOI: 10.17103/reei.29.07

Con Internet todo esto ha cambiado. Prácticamente todas las organizaciones terroristas que disponen de cierta infraestructura cuentan con páginas web y otros canales de transmisión de comunicación a través de la red, que les facilitan enormemente el trabajo de reivindicación de acciones, explicación de móviles, diseminación de propaganda, glorificación del terrorismo, incitación para nuevos actos entre los posibles lectores, lanzamiento de amenazas, reclutamiento de personal, búsqueda de financiación, comunicación entre los miembros, con los medios y con el público en general[27].

Con el anonimato prácticamente asegurado, el potencial de audiencia que supone este tipo de páginas web supera enormemente cualquier previsión de alcance de los canales tradicionales y, además, escapan fácilmente al control de una posible censura[28].
Los recursos necesarios para llevar a cabo toda esta publicidad también son mucho más reducidos. Antes sólo algunas organizaciones eran capaces de publicar periódicos, revistas o programas de televisión, y menos aún, con cierta regularidad; ahora Internet es potencialmente accesible para todo aquel que quiera y con un modesto presupuesto. Las organizaciones terroristas pueden colar fácilmente sus opiniones y puntos de vista, así como sus amenazas en la red, incrementando a su vez las posibilidades de que sus contenidos sean luego utilizados por los medios de comunicación tradicionales, ya que éstos echan mano frecuentemente de Internet como fuente de material.

Si hablamos de reclutamiento y entrenamiento, Internet de nuevo ofrece numerosos atractivos al terrorismo. Las "ofertas" se cuelgan y se dejan fácilmente accesibles desde varios portales, quedando garantizado un amplio público.

De la misma manera, dar por Internet detalles de cuentas bancarias, ofrecer *merchandising* (libros, CDs, camisetas, etc.), así como establecer links publicitarios o de otras organizaciones terroristas contribuye a lograr financiación para el terrorismo.

Pero Internet también puede ser usado con otros propósitos, desde la búsqueda de información sobre objetivos (datos personales, detalles empresariales, imágenes de satélites, planos de edificaciones, paseos virtuales por distintos lugares, etc.), hasta la planeación de atentados. En la red se pueden encontrar instrucciones para hacer bombas, consejos para saber dónde colocarlas, recetas para realizar venenos caseros, explicaciones para desarrollar técnicas guerrilleras o manuales para secuestrar rehenes.
Por último, los terroristas utilizan la red de forma habitual para su comunicación confidencial. El uso de las nuevas tecnologías para mantener contacto entre los terroristas disfruta de muchas de las ventajas que ya han sido señaladas: es barato, rápido, muy a menudo anónimo y ampliamente accesible. Además, desde que es posible la encriptación de datos y el empleo de la esteganografía también es más seguro, aunque los mensajes viajen por redes públicas. Si decíamos que la propaganda requiere amplia

[27] Véase GEBAUER, I., *Cyberjihad, virtuelle Umma oder Islam online?*, Diplom.de, Hamburg, 2009.
[28] Por supuesto que muchas de las páginas terroristas son objeto de medidas de contraterrorismo por parte de agencias gubernamentales que tratan de identificarlas y hacerlas inaccesibles, pero las organizaciones terroristas siempre tratarán de burlar el control oficial, inventando nuevas vías para llegar al público. Por ejemplo, un video con propaganda de contenidos terroristas puede aparecer camuflado en YouTube poniéndole como banda sonora una canción pop de moda en ese momento.

DOI: 10.17103/reei.29.07

visibilidad, la comunicación entre terroristas depende de un buen camuflaje y canales fiables de transmisión[29]. Cabe reiterar que en casi cualquier parte del mundo se puede tener acceso a Internet a través de un teléfono móvil.

Por último, no debemos olvidar que junto a los riesgos actuales, es necesario estar preparados para los futuros. El mundo de la tecnología avanza a pasos agigantados y no cabe duda de que debemos adelantarnos al posible uso que los terroristas hagan de los sistemas electrónicos que tienen a su alcance.

2. La propaganda on-line del Estado Islámico

La propaganda por la acción, descrita por primera vez por la federación italiana de la Internacional Anarquista en 1876 aludía a los actos terroristas como el medio propagandístico más eficaz, y el más adecuado para llegar hasta las capas sociales más profundas[30].

Como ya hemos puesto de relieve, el éxito de la ofensiva del EI se debe en gran medida a su poderío militar, pero también a una cuidada estrategia en otros ámbitos, uno de los cuales es precisamente el de la comunicación[31]. Respecto a este último, el EI está realizando una agresiva campaña de propaganda, a través de diversos medios de difusión y fundamentalmente utilizando las redes sociales[32]. Sus macabras acciones han captado la atención de los medios y del público en general, asegurándose un espacio publicitario sin parangón cuando nos referimos a organizaciones yihadistas que operan casi en exclusiva en los países musulmanes.

Podemos señalar tres objetivos principales de la propaganda online del EI: a) mostrar, reivindicar, ensalzar y justificar sus acciones, b) reclutar nuevos miembros y forjar alianzas con otras organizaciones, y c) amenazar con cometer nuevos actos terroristas en cualquier parte del mundo.

Comencemos con la utilización de Internet para el encumbramiento de los logros conseguidos, enfocada a intensificar el apoyo a la organización. El EI muestra a través

[29] Han sido detectadas dos técnicas para camuflar mensajes entre los terroristas. La primera consiste en ocultar mensajes en fotos que se cuelgan en conocidas páginas web. El público en general sigue contemplando una foto sin sospechar nada, mientras que los terroristas receptores del mensaje lo descifran y acceden a él (*esteganografía digital*). La segunda estriba en usar cuentas gratuitas de e-mail, con una contraseña que conocen dos o más personas y que permite escribir un mensaje, guardándolo en borrador sin enviarlo. El receptor o receptores entran en la misma cuenta con la contraseña que conocen de antemano y lo leen. En ambos supuestos, para más seguridad también se puede encriptar el contenido de los mensajes.

[30] El anarquista Piotr Kropotkin decía que una sola acción terrorista era capaz, en unos pocos días, de hacer más propaganda que miles de panfletos.

[31] Barrancos señala que donde el EI ha logrado profesionalizarse ha sido en el ejercicio de su auténtico trabajo: el terrorismo y su difusión; BARRANCOS, D., "Los community managers del terror: la propaganda online de ISIS y su ofensiva sobre Irak", *Boletín Electrónico del IEES*, nº 82bis, 2014, p. 5.

[32] Mantener el contacto entre militantes o realizar *merchandising* a través de Facebook, mostrar los lujos, experiencias y momentos llenos de adrenalina en la vida de los yihadistas por medio de Instagram o lanzar campañas de apoyo al EI en Twitter, son "ciberactividades" a la orden día en esta organización.

DOI: 10.17103/reei.29.07

de imágenes y videos los territorios que actualmente están bajo su control tanto en Siria como en Irak, pero además los envuelve en un halo de normalidad. El mensaje es que la pacificación de esas zonas se ha conseguido con el triunfo del EI. Gracias a ello, la población civil goza de una estructura política y administrativa que se encarga de dar respuesta a sus necesidades de alimento, educación, seguridad, etc.

A su vez, se muestra cómo el orden establecido no tiene la potencia que se le supone. Por un lado, se ha dejado en evidencia al gobierno iraquí, cuyas fuerzas de seguridad han sido entrenadas y armadas por Estados Unidos. Por el otro, el EI en Siria se ha revelado como la única milicia de las enfrentadas al régimen de Bashar al-Assad capaz de apoderarse de forma perdurable de parte del territorio.

Esa sería la cara más amable de la apología que realiza en la red, porque el EI también expone otro tipo de "logros", esta vez reprobables desde el punto de vista jurídico-internacional. Se encuentran videos –por cierto, de gran calidad técnica- en los que se muestran operaciones militares grabadas desde las mirillas de los rifles de los francotiradores, explosiones a cámara lenta, tomas aéreas y en diferentes planos, etc., que no solo sirven para vanagloriar los éxitos del movimiento, sino también para infundir miedo en los que se oponen a él[33].

Así mismo, el EI publica un informe anual (al-Naba) donde recoge todas las acciones militares y terroristas llevadas a cabo, las analiza y se marca objetivos para el próximo ejercicio. Allí se relacionan las distintas clases de ataques y se contabilizan las acciones en cada categoría: atentados con coches bomba, atentados suicidas, ofensivas armadas, asesinatos con armas con silenciador o armas blancas, asaltos con mortero, casas y templos volados o quemados, muertos por francotirador, ciudades ocupadas y liberadas de los infieles, personas expulsadas, prisioneros liberados, etc.[34]

Aunque sin duda los materiales más conocidos son los videos y fotografías que circulan por Internet donde los terroristas del EI muestran decapitaciones, ejecuciones en masa, tratos degradantes infligidos a soldados capturados o a civiles chiíes o kurdos, entre otras atrocidades. A su vez este material es compartido y comentado a través de las redes sociales como Facebook, Twitter o Instagram y otras webs, cuyos *community managers* se encargan de incitar al debate, controlar los tiempos y mantener viva la comunicación, incardinándola hacia sus objetivos estratégicos y operativos.

El segundo fin señalado hace alusión al reclutamiento de nuevos yihadistas por todo el mundo y la consecución de alianzas con otras organizaciones que operan en Oriente Medio.

[33] Un vídeo de estas características titulado *The Claging of the Swords IV* ha sido comparado con la película de Hollywood *La noche más oscura*; MALTERRES, S. / NASR, W., "ISIS jihadist put out Hollywood-style propaganda film", *France 24 – The Observers*, 2014, p. 2

[34] De momento, existen dos informes, 2013 y 2014, y se pueden consultar en http://azelin.files.wordpress.com.

DOI: 10.17103/reei.29.07

Captar nuevos combatientes es de suma importancia para una organización relativamente pequeña si tenemos en cuenta su ambición de dominar un territorio con un número de habitantes muy elevado. En este sentido, el reclutamiento de ciudadanos en países occidentales para luchar junto al EI es una de las mayores preocupaciones de los gobiernos al tratarse de individuos con libertad de movimiento y que, por tanto, podrían perpetrar atentados fuera de las fronteras del Islam[35].

Como ya hemos apuntado, en occidente a los musulmanes incluso de segunda y tercera generación en estos momentos les resulta mucho más atractivo el EI que Al Qaeda. Jóvenes descendientes de inmigrantes procedentes de países islámicos que residen en Europa, Australia, Canadá o Estados Unidos atraviesan una profunda crisis de identidad. Conscientes de ello, las organizaciones yihadistas, siempre dispuestas a explotar este filón, ofrecen una propuesta tentadora[36]. El EI, concretamente, brinda algo más que la pertenencia a una organización consagrada a la lucha por el Islam: presenta una sociedad yihadista dentro de un Califato con territorio reducido pero con visos de expansión. Esa sociedad ya existe, goza de un orden social, un sistema político y una estructura militar, y está abierta a todos esos musulmanes que no se reconocen en las comunidades occidentales donde ahora residen. Se ofrece una mutualidad apoyada en la colaboración de todos los socios que redunda ya en la creación de un verdadero Estado donde reiniciar sus vidas, incluso emigrando en familia. Sin duda, el éxito cosechado en territorio sirio e iraquí engendra motivaciones individuales para la implicación en actividades yihadistas con criterios de racionalidad[37].

Por otro lado, la concepción menos tolerante con lo que denominan sectas islámicas desviadas o el resentimiento hacia quienes consideran infieles o apóstatas, levanta pasiones entre jóvenes y no tan jóvenes musulmanes que desde diversos puntos del mundo optan por la militancia. Incipientes organizaciones en Libia, Jordania, Argelia, Yemen o Túnez, entre otros, parecen interesadas en la concepción del Islam que hace el EI y, por tanto, no les costará sellar alianzas de cara a su desarrollo en otros países musulmanes.

[35] Precisamente, la justicia estadounidense acusó al joven Mufid A. Elfgeeh, yemení nacionalizado estadounidense, de reclutar militantes para luchar en las filas del EI en Siria e Irak y atentar contra musulmanes chiíes y militares en el país norteamericano. En España se han desmantelado de momento dos redes de captación de mujeres jóvenes, a través de WhatsApp y Facebook, que actuaban en Ceuta y Melilla con el fin de conseguir guerreras yihadistas y compañeras sentimentales para los muyahidines que combaten en Siria e Irak, más otra red de reclutamiento de hombres también en Ceuta.

[36] En junio de 2014 fue detenido el ciudadano español Hamido Hamido Mohamed. En su auto de prisión, el juez le acusaba de un delito de enaltecimiento del terrorismo, entre otros. El auto explica que Hamido lanzaba comentarios en contra de los "infieles" tendentes a su exterminio y asesinato y manifestaba su voluntad de morir como mártir, ya sea incorporándose a grupos terroristas en otros países o pasando a la acción matando "infieles". "Pido a Allah que me dé valor de matar Tasut (siglas utilizadas por los islamistas radicales para referirse a los occidentales)", escribió en su perfil de Facebook en junio de 2012.

[37] Asegura Reinares que “este tipo de motivaciones se interiorizan mediante el proceso de radicalización, a lo largo del cual se adquieren las actitudes y creencias propias del salafismo yihadista, que justifican en términos tanto morales como utilitarios el uso de la violencia y el terrorismo, supuestamente para defender y expandir el islam”; artículo de prensa aparecido en *El País*, el 9 de septiembre de 2014.

DOI: 10.17103/reei.29.07

A su vez, la reacción de Estados Unidos y otros países occidentales bombardeando posiciones del EI, despierta el espíritu rebelde, lo que provocará la incorporación de más adeptos dispuestos a llevar a cabo nuevas acciones individuales o colectivas. Una parte de los islamistas, no todos, verán a los rebeldes como héroes, a pesar de los actos de barbarie cometidos[38]. Evidentemente sin el despliegue de propaganda online y sin el amplio tratamiento mediático del movimiento, el EI nunca habría conseguido sumar tantas simpatías y adhesiones.

Por último, tenemos que considerar la amenaza de cometer nuevos actos terroristas en cualquier parte del mundo[39]. Las organizaciones terroristas pueden colar fácilmente sus opiniones y puntos de vista, así como sus amenazas en la red, incrementando a su vez las posibilidades de que sus contenidos sean luego utilizados por los medios de comunicación tradicionales.

El material gráfico que circula por Internet, así como las noticias que se transmiten por los medios de comunicación, contienen acciones sanguinarias y destructivas. Las amenazas lanzadas online de la repetición de esos y otros actos, acaparan la atención de esos mismos medios, a la vez que circulan y son comentadas en numerosas redes sociales. El efecto intimidatorio se multiplica provocando el pánico de soldados y población civil. Sea por miedo o fascinación ante la violencia, muchos soldados desertan y se unen a las fuerzas combatientes del EI. El terror ejercido sobre la población civil hace que no oponga resistencia, subyugándose a las nuevas autoridades o huyendo antes de que tomen el control de su ciudad o aldea.

Estos son los logros obtenidos por el EI a través de su propaganda online; ahora es el momento de preguntarnos si paralelamente a la intervención militar contra el EI en el espacio físico, es posible llevar a cabo una ofensiva en el espacio cibernético y cuáles son las cuestiones jurídicas que se plantean.

IV. LA COMPLEJIDAD DEL DISEÑO LEGAL DEL CIBERESPACIO

1. Las especiales características del ciberespacio

La libertad ha sido hasta el momento el principal valor a preservar en el ciberespacio. Sin embargo, esa libertad no puede desarrollarse en todo su potencial si no se despliega en un entorno seguro. Por ello, más que limitar la libertad digital, las acciones contra

[38] La elección de objetivos que se podrían considerar “legítimos” (dirigentes de los países “invasores”, miembros del gobierno instaurado por estos, mercenarios extranjeros), junto a la demostración de ciertos límites morales, aumentaría sin duda la receptividad del mensaje que el EI quiere hacer llegar a todos los musulmanes del mundo. Eso sí, tendría menos impacto propagandístico.

[39] Diversos países reforzaron la seguridad en sus principales puntos turísticos después de que el EI hiciera un llamamiento en foros de internet a los "lobos solitarios" que residen en EEUU y Europa para que atenten en lugares concurridos con artefactos caseros. Para las autoridades estadounidenses, la mayor amenaza no es que células del EI o de Jorasán puedan desplazarse para atacar en Estados Unidos, sino la capacidad de los yihadistas para inspirar la actuación de esos "lobos solitarios" en sus países de residencia.

DOI: 10.17103/reei.29.07

contenidos ilegales y dañinos en la red, reafirman la idea de un infouniverso libre de fiscalización pero protegido.

Internet es una red global que comprende infinidad de redes individuales. La representación visual de la información en Internet se ofrece a través de páginas digitales dentro de sitios web. La World Wide Web es accesible a través de los identificadores de nombres de dominio y las direcciones de sitio, usando motores de búsqueda. Los nombres de dominio se alojan por un sistema centralmente coordinado de registros bajo los auspicios de la Internet Corporation for Assigned Names and Numbers (ICANN)[40].

Por eso se dice que la arquitectura de Internet es tridimensional, esto es, posee un sistema jerárquico de registros de dominio, donde proliferan los intermediarios de diversa naturaleza que, a su vez, "controlan" los accesos, los protocolos y los servidores. Estos últimos muchas veces se sitúan en distintos países, lo que dificulta el rastreo, y si esos países poseen una legislación más laxa en materia de cibercrimen, también resulta arduo el enjuiciamiento de los hechos.

En cualquier comunicación vía Internet nos encontramos con un número importante de participantes o actores. Por ejemplo, en toda interacción en el ciberespacio hay alguien que ha subido la información a la red, alguien que se la baja, el portal que permite el acceso o el visionado de esa información, el servidor que contiene los archivos de la página web, la ruta de acceso a los datos a través de nodos que conectan todo el mundo, las distintas partes que constituyen la página web (como imágenes, archivos de voz, videos) que se incorporan desde otros servidores, links hacia otras páginas web, y la intervención de los operadores de sistema. Dada la naturaleza transnacional de las comunicaciones telemáticas, es muy difícil de probar la jurisdicción competente tanto para conocer de las controversias civiles como para perseguir los ciberdelitos, porque todos estos actores y actividades pueden estar "localizados" en diferentes jurisdicciones[41].

Además, en demasiadas ocasiones los datos circulan de manera anónima y sin que se pueda determinar con exactitud cuál es la regulación aplicable, si es que la hay, ni la jurisdicción que la debe controlar[42].

[40] Se trata de una corporación sin fines de lucro responsable de administrar el sistema de números de protocolos de Internet (IP), el sistema de nombres de dominio (DNS), y otros protocolos de Internet relacionados.

[41] LONGWORTH, E., "The Possibilities for a Legal Framework for Cyberspace – Including a New Zealand Perspective", en FUENTES-CAMACHO, T. (ed.), *The International Dimensions of Cyberspace Law*, Ashgate – UNESCO, Aldershot, 2000, p. 36.

[42] El coste de monitorizar las conductas que se despliegan a través de la red es muy alto. El sistema descentralizado de control conlleva que si el contenido de un servidor es incompatible con la legislación de un determinado Estado, puede cambiarse con relativa facilidad a cualquier otro sitio del ciberespacio fuera de la jurisdicción de ese Estado. Véase POST, D.G., "Anarchy, State and the Internet: An Essay on Law-Making in Cyberspace", *Journal of Online Law*, Article 3, 1995, p. 17.

DOI: 10.17103/reei.29.07

La facilidad del anonimato y, lo que es más, la posibilidad de ocultar el origen de los mensajes o de introducirlos a través de portales situados en cualquier parte del mundo evitando la responsabilidad legal que pudiera surgir en países cuya legislación castiga determinadas conductas, son otras de las características a tener en cuenta a la hora de desarrollar un cuerpo de normas que regulen el ciberespacio. Internet permite cambiar de jurisdicción con relativa facilidad o escapar de los "controladores", sean estos intermediarios o los propios Estados.

Por otro lado, la información digital no tiene un soporte material estable en el espacio y en el tiempo. La irrelevancia de las fronteras geográficas, lo mismo que la posibilidad de rescatar y poner al día en cualquier momento esa información, son características del ciberespacio que van a tener un impacto en el diseño de la legislación aplicable.

Los problemas surgen de la extraterritorialidad de las actividades y de la aplicación extraterritorial de las normas nacionales. En muchas ocasiones esa aplicación extraterritorial o justificar la jurisdicción sobre los efectos de esas actividades no va a ser posible.

En este sentido, existe una falta de congruencia entre el carácter transnacional del ciberespacio, la irrelevancia de las fronteras geográficas en el mismo, y la limitación de aplicación de la ley y de la jurisdicción de los tribunales[43]. Las normas que se basan en criterios territoriales, son manifiestamente ineficaces en el entorno virtual. Post asegura que "Internet no es meramente multi-jurisdiccional, sino casi a-jurisdiccional"[44].

El ciberespacio clama por nuevas normas, desligadas de la jurisdicción territorial, que puedan servir en distintos espacios online, para gobernar un amplio espectro de fenómenos que no tienen un claro paralelismo en el mundo físico. Las cuestiones del ciberespacio demandan una redefinición de la creación y de la aplicación de la ley. Los conceptos y prácticas jurídicas tradicionales se enfrentan al desafío de un entorno de comunicación no familiar y extremadamente cambiante, donde la información adquiere su valor si se transmite, no si se controla y se censura.

Todas estas características subvierten el poder de las autoridades locales para gobernar los comportamientos en la red. La estructura vertical y asimétrica de Internet tiene un fuerte impacto en su regulación, por lo que a veces resulta más fácil para los proveedores del servicio que para las autoridades gubernamentales imponer condiciones a los usuarios[45].

[43] Johnson y Post afirman lo siguiente: "Cyberspace radically undermines the relationship between legally significant (online) phenomena and physical location. The rise of the global computer network is destroying the link between geographical location and: (1) the power of local governments to assert control over online behavior; (2) the effects of online behavior on individuals or things; (3) the legitimacy of the efforts of the local sovereign to enforce rules applicable to global phenomena; and (4) the ability of physical location to give notice of which sets of rules to apply"; JOHNSON, D.R. and POST, D.G., "Law and Borders: The Rise of Law in Cyberspace", *Stanford Law Review*, 48, 1996, p. 3.

[44] POST, "Anarchy, State and the Internet…", op. cit., p. 15.

[45] La UE ha tratado de "persuadir" a las grandes compañías tecnológicas (Facebook, Twitter, Google y Microsoft) para que ayuden a detectar contenidos ciberterroristas y, más allá de aislar los mensajes en

DOI: 10.17103/reei.29.07

Todo ello lleva a muchos autores a abogar por un marco legal descentralizado que se base en la voluntaria aceptación de estándares o protocolos técnicos y en formas alternativas de resolución de conflictos. Según Longworth la emergencia de una toma de decisiones descentralizada podría muy bien proporcionar una forma de gobernanza del ciberespacio más coherente, compresiva e identificable que la regulación convencional emanada de una autoridad superior centralizada[46].

Sin embargo, las dificultades en torno a la jurisdicción y aplicación de la ley en Internet no son insalvables, solo hace falta un enfoque multilateral o multidimensional que responda al grado de sofisticación que requiere la red en términos de diseño legislativo[47].

2. Formas de regulación del ciberespacio y su aplicación al ciberterrorismo

De acuerdo con la doctrina predominante, las principales formas de regulación de las conductas en el ciberespacio son cuatro: las normas jurídicas, las normas sociales, el mercado y el código.

Las normas jurídicas directas surgidas de las autoridades legislativas correspondientes suelen tener que ver con conductas penalmente reprochables: la violación de los derechos de autor, la difamación o la pornografía infantil entrarían en esta categoría de conductas para las que existen leyes sustantivas que buscan la averiguación, persecución y sanción de los delitos cometidos por medios informáticos.

Las normas sociales amenazan con una sanción que vendrá impuesta, de forma descentralizada, por la sociedad o la comunidad en cuestión. La presión social -o la práctica del "flaming"- significa que los demás usuarios a los que no les gusta el comportamiento de un participante en una red o comunidad, pueden protestar masivamente contra esta persona inundando el sitio de mensajes de protesta. Este comportamiento disuadiría las conductas ilegales y alentaría la integridad en la red.

El mercado compele a individuos y grupos a adoptar determinadas conductas y no otras, pero este tipo de regulación se aplicará a las transacciones económicas y a las prestaciones de servicios.

Y, por último, el código se refiere a las normas derivadas de la propia naturaleza y arquitectura del ciberespacio, esto es, a aquellas condiciones que aparecen en los

---

cuestión, los pongan en conocimiento de las autoridades locales para que actúen en consecuencia. Artículo de prensa aparecido en *El País*, el 7 de octubre de 2014.

[46] LONGWORTH, "The Possibilities for a Legal Framework for Cyberspace…", op. cit., p. 18.

[47] Grainger afirma que "no domain coming within the reach of humans has yet resisted the human urge to explore, occupy, civilize and govern"; GRAINGER, G., "Freedom of Expression and Regulation of Information in Cyberspace", en Fuentes-Camacho, Teresa (ed.), *The International Dimensions of Cyberspace Law*, Ashgate – UNESCO, Aldershot, 2000, p. 119.

DOI: 10.17103/reei.29.07

protocolos de acceso y uso de la red[48]. Lessig afirma que el software (o los diseñadores del código) están definiendo las obligaciones que se aplican a los usuarios de estos servicios y tecnologías. Por ello, los códigos para diferentes arquitecturas expresan distintos valores[49]. Eso sí, las autoridades estatales siempre tendrán la oportunidad de influir indirectamente en ese código, transmitiendo a través de su normativa los principios que deseen proteger[50].

Descentralización, multidimensión y jerarquía son ingredientes básicos de la receta que ha dado lugar a la red de redes. Internet tiene un modelo descentralizado de gobernanza que es el predominante y parece que lo seguirá siendo en el futuro[51], posee un gran número de intermediarios que operan en Internet, dando servicios de transmisión, direccionando y recibiendo mensajes, y responde a una jerarquía vertical en la que proveedores de servicio (ISPs) y operadores de sistema (sysops) se clasifican en distintos niveles. A pesar de estas características y del grado de sofisticación que requiere, el Derecho del ciberespacio se va a ver influido innegablemente por los valores defendidos por los Estados.

Si bien es cierto que la intervención legislativa directa de los poderes públicos estatales plantea el problema de su localidad, no nos cabe duda de que en cuestiones que tienen que ver con conductas delictivas la regulación debe responder a este tipo de normativa. Evidentemente, como sugeriremos más adelante, estas normas jurídicas directas a su vez deberían responder a un mandamiento de una organización internacional para que todos los países tengan regulación y la misma se adecúe a las pautas dadas por la organización.

Evidentemente las otras formas de regular el ciberespacio pueden ayudar pero no sirven por sí solas para prevenir y sancionar los comportamientos delictivos que pueden tener lugar en la red, entre ellos el ciberterrorismo. Evidentemente una obligación directa incluida en una norma jurídica es mucho más efectiva para ejercer control.

Algunas voces advierten que cuando se quiere seguir una particular política o alcanzar un determinado valor en el ciberespacio, se cae de nuevo en la intervención legislativa de los poderes públicos para reflejar esos valores o esas políticas y que una intromisión de estas características puede constreñir el propio diseño y la forma que tiene de operar

[48] LESSIG, L., "The Law of the Horse: What Cyberlaw Might Teach", *Harvard Law Review*, 113-2, 1999, p. 504. Véase también LESSIG, L. and LUCZKOW, J.L., *Code and Other Laws of Cyberspace*, Basic Books, New York, 1999 y LESSIG, L., *Code 2.0*, Basic Books, New York, 2006.

[49] LESSIG, "The Law of the Horse…", op. cit., p. 515.

[50] Ejemplos de esta normativa los encontramos en la legislación sobre protección de datos o en las normas sobre telecomunicaciones.

[51] Se suele hacer referencia a "autogobernanza", "autoregulación" o, incluso, "autocontrol". Johnson y Post lo explican de la siguiente manera: "De facto rules may emerge as a result of a complex interplay of individual decisions by domain name and IP address registries (regarding what conditions to impose on possession of an online address), by sysops (regarding what local rules to adopt, what filters to install, what users to allow to signo n, and with which other systems to connect) and by users (regarding which personal filters to install and which systems to patronize)"; JOHNSON, D. and POST, D., "And How Shall the Net B Governed? A Meditation on the Relative Virtues of Decentralized Emergent Law", in KAHIN, B. and KELLER, J. (eds.), *Coordinating the Internet*, MIT Press, Cambridge, 1996, p. 3.

DOI: 10.17103/reei.29.07

Internet. Por eso, se aconseja que esta forma de regulación del ciberespacio sea muy limitada en su aplicación[52].

No obstante, el Estado está en la necesidad de intervenir cuando la desregulación presente en la red puede poner en riesgo el orden público, los derechos y las libertades fundamentales de sus ciudadanos o los valores esenciales del Estado. Aunque en muchos aspectos Internet va a estar regido por un sistema de autoregulación no coordinado y descentralizado, las conductas criminales cometidas en el ciberespacio deberían reglamentarse a través de normas positivas, como lo hacen las que se desarrollan en el mundo físico. Es evidente que, además, dichas normas se deberían adaptar o reformar para poder influenciar la autorregulación y la estandarización técnica del ciberespacio. Como señala Post, si la red funciona como un portero para los usuarios del ciberespacio, se espera que los poderes públicos traten "to impose coercitive sanctions on network administrators (and thereby on the network rules) in order to implement their own particular preferred set of rules on behaviour in this environment"[53].

V. DIMENSIÓN INTERNACIONAL DEL CIBERTERRORISMO

1. Regulación internacional y armonización de legislaciones internas como respuesta al ciberterrorismo

Como ya hemos puesto de relieve anteriormente, la libertad ha sido hasta el momento el principal valor a preservar en el ciberespacio. Sin embargo, esa libertad no puede desarrollarse en todo su potencial si no se despliega en un entorno seguro.

Algunos Estados y organizaciones regionales han legislado sobre los problemas planteados en el ciberespacio[54]. Sin embargo, esas regulaciones no alcanzan a dar respuesta a dichos problemas desde el momento en que las actividades cibernéticas, lícitas o ilícitas, no conocen de fronteras.

Conviene recalcar que para lo bueno y para lo malo, la interconectividad que nos brinda Internet ha llegado para quedarse e incrementarse, con lo que su regulación no puede configurarse en compartimentos estancos que respondan a las reglas tradicionales de cooperación judicial internacional. Por ello, parece que la solución vendría dada a través

[52] LONGWORTH, "The Possibilities for a Legal Framework for Cyberspace…", op. cit., p. 27.
[53] POST, D.G., "Anarchy, State and the Internet…", op. cit., p. 31.
[54] El Consejo de Europa posee algunos instrumentos de suma importancia para la protección frente a la cibercriminalidad y frente al terrorismo: Convención Europea sobre Cibercrimen de 2001, Convención Europea sobre Prevención del Terrorismo de 2005 y Convención relativa al blanqueo, seguimiento, incautación y decomiso de productos del delito y sobre financiación del terrorismo de 2005. De la conjunción de estas convenciones y la adaptación de la legislación interna de los Estados miembros a las mismas, a nivel regional europeo se puede asegurar una protección eficaz frente a las actividades ciberterroristas; CHICHARRO, A., "La labor legislativa del Consejo de Europa frente a la utilización de Internet con fines terroristas", *Revista de Internet, Derecho y Política*, nº 9, 2009, p. 12.

DOI: 10.17103/reei.29.07

de una regulación internacional de las actividades terroristas y, por ende, ciberterroristas.

Antes de abogar por el desarrollo de una normativa internacional que regule el ciberespacio, hay que preguntarse si es deseable o factible una regulación de este tipo y si interesaría la adopción de un tratado o más bien el despliegue de una macro-estrategia para todas las normas que toquen o hayan sido afectadas por el advenimiento de Internet.

El problema con el que nos encontramos cuando apelamos a la concertación de un tratado internacional es que el proceso de adopción suele ser muy lento, mientras las tecnologías de la información y la comunicación están en constante cambio. Por ello, cualquier norma uniforme tiene que ser "tecnológicamente neutral", esto es, debe redactarse de tal manera que no solo sea aplicable a los problemas surgidos del progreso en el momento de la adopción del instrumento internacional, sino que sirva para adaptarse a los rápidos y continuos avances en este campo.

Aunque el desarrollo convencional sea la vía más adecuada, sus disposiciones pueden combinar normas sustantivas legalmente exigibles con otras más flexibles que incluyan principios generales allí donde se necesite una mayor capacidad de adaptación al adelanto técnico o donde el consenso entre Estados sea más difícil de alcanzar. Se trataría de combinar preceptos de *hard law* con disposiciones de *soft law* material. En este último caso, la norma jurídicamente vinculante existe y es imperativa, lo que ocurre es que está formulada con principios generales o sin especificar obligaciones concretas desde el punto de vista sustancial[55]. Allí donde es más probable que exista un consenso entre los Estados de la comunidad internacional podrían incluirse normas rígidas en cuanto a su vinculación jurídica; pero allí donde existan puntos de discrepancia o mayor volatilidad debido al progreso tecnológico las normas de *soft law* podrían intentar apelar a la coordinación de legislaciones internas en la materia dejando un mayor margen de maniobra a los Estados.

Quizás ese tratado, además de incluir normas sustantivas que regulen el ciberterrorismo, promoviendo la armonización de legislaciones para toda la comunidad internacional, también podría aclarar las cuestiones jurisdiccionales.

Parece importante que no solo se adopten normas para prohibir las conductas ciberterroristas, sino que además cuando se vulneren las mismas no existan obstáculos a la hora de determinar la autoridad judicial que va a conocer del asunto. Una obligación de los Estados de juzgar o extraditar (*aut dedere aut judicare*) a las personas autoras de estos delitos que se encuentren en su territorio, tal y como se ha incluido en muchos de los instrumentos sectoriales contra el terrorismo internacional, parece perfectamente adecuada también para el ciberterrorismo.

[55] Véase ABOTT, K. and SNIDAL, D., "Hard Law and Soft Law in International Governance", *International Organization*, June, 2000, p. 423.

DOI: 10.17103/reei.29.07

Recordemos que la opción por instrumentos internacionales no es nueva en materia de terrorismo. Si bien es cierto que nunca se ha podido alcanzar un consenso suficiente para promover un tratado general sobre la materia, no podemos olvidar que existen regulaciones en sectores concretos que han logrado frenar determinados actos relacionados con el fenómeno terrorista.

A partir de los años sesenta, se adoptaron varias convenciones con el propósito de acabar con los reiterados secuestros de aeronaves y barcos por parte de distintas organizaciones terroristas[56]. Ya en los noventa, la utilización de bombas y otros materiales altamente peligrosos en los ataques perpetrados dio lugar a otra remesa de tratados sobre esta cuestión sectorial[57]. Y por último, la financiación del terrorismo –aspecto difícil de consensuar a nivel internacional- también ha sido concertada globalmente[58].

Con mayor o menor éxito entre los Estados en cuanto a prestación del consentimiento en obligarse por estos tratados, lo cierto es que el esfuerzo de consenso se ha realizado y, pese a los cambios producidos en la sociedad internacional, continúan siendo instrumentos de suma importancia para lucha contra el fenómeno terrorista. Por ello, tras los atentados del 11-S, el Consejo de Seguridad en su Resolución 1373 (2001) demandaba la ratificación de todos los instrumentos internacionales contra el terrorismo aprobados por la Asamblea General[59].

Evidentemente si se producen reiterados llamamientos a la adhesión a los convenios sectoriales sobre terrorismo es porque todavía existen algunos Estados reticentes a obligarse por tratados internacionales en esta materia. Sin embargo, otros muchos están dispuestos a prestar su consentimiento y, posteriormente, a cumplir con las obligaciones impuestas en los mismos, lo cual no deja de ser positivo. Si en el mundo físico se ha conseguido, cuando la amenaza provenga del espacio virtual también se podría enfrentar a través de un instrumento internacional con las características que ya hemos avanzado a grandes rasgos.

---

[56] Sobre navegación aérea disponemos del Convenio de Tokio sobre las infracciones y ciertos actos cometidos a bordo de aeronaves de 1963, del Convenio de La Haya para la represión del apoderamiento ilícito de aeronaves de 1970, del Convenio de Montreal para la represión de actos ilícitos contra la seguridad de la aviación civil de 1971 y del Protocolo para la represión de actos ilícitos de violencia en los aeropuertos que presten servicio a la aviación civil internacional de 1988. Sobre navegación marítima tenemos el Convenio sobre la seguridad de la navegación marítima y el Protocolo sobre plataformas fijas, ambos de 1988.

[57] Sobre este particular, existen varios instrumentos: la Convención sobre los materiales nucleares de 1980, el Convenio sobre los explosivos plásticos de 1991, el Convenio sobre los atentados terroristas con bombas de 1997 y el más reciente Convenio internacional para la represión de los actos de terrorismo nuclear de 2005.

[58] Nos referimos al Convenio Internacional para la represión de la financiación del terrorismo de 1999.

[59] Tras la condena sin paliativos de dichos atentados en su Resolución 1368 (2001) del día después del cruento ataque, el Consejo de Seguridad adoptó la Resolución 1373 (2001), de 28 de septiembre de 2001, que impone obligaciones generales a los Estados miembros para criminalizar el terrorismo y recomienda la adopción de una serie de conductas en el ámbito de la cooperación internacional contra el fenómeno, abarcando desde la colaboración de servicios policiales y de inteligencia hasta la que tiene lugar entre los aparatos judiciales, al tiempo que pide la ratificación de todos los instrumentos internacionales contra el terrorismo aprobados por la Asamblea General.

DOI: 10.17103/reei.29.07

En cualquier caso, siempre habrá una minoría de Estados que no estarán de acuerdo con los valores proyectados o los intereses salvaguardados en un texto de estas características y que no aceptarán las posibles sanciones. Si no se da una aplicación universal, hay que ser consciente de que los usuarios pueden buscar operar desde uno de estos "paraísos cibernéticos". A pesar de ello, los Estados siempre estarán interesados en facilitar el acceso a las actividades en la red, preservando la propia seguridad y la de sus ciudadanos, lo que puede arrastrarles a participar en la negociación y adopción de un instrumento universal, lo mismo que a la posterior prestación de su consentimiento en obligarse por él.

En cualquier caso, abogamos por un instrumento relativamente general por dos motivos: en primer término, porque es más fácil llegar a un consenso cuando no se regulan cuestiones de detalle y, en segundo, porque en un mundo tan diverso y rápidamente cambiante, dar soluciones precisas a los problemas específicos abocaría al instrumento a una obsolescencia prematura haciéndolo ineficaz.

2. Problemas que plantea la adopción de un tratado internacional para luchar contra el ciberterrorismo

Si la solución avanzada aboga por un instrumento internacional convencional promovido por una organización universal, que contenga disposiciones lo suficientemente genéricas para que se establezcan los principios y valores del Derecho del ciberespacio, sin limitarlo en su aplicación a la tecnología actual, habría que plantearse cuáles son los problemas que la obstaculizan.

Comencemos por algo que puede suponer una obviedad: no concurre la voluntad por parte de los Estados que conforman la comunidad internacional de convenir una normativa que permita, una vez adaptada la legislación interna, prevenir, reprimir y sancionar de forma equivalente estas conductas en cualquier parte del mundo.

La primera razón que podríamos apuntar para esa falta de voluntad radica en que el Derecho Penal sigue siendo un bastión de la soberanía estatal. Sí que existen casos en los que la dimensión transnacional de determinados ilícitos ha llevado a los Estados a acordar tratados en cuestiones criminales como la trata de personas, el tráfico de armas, el tráfico de drogas, el blanqueo de capitales o la corrupción; y el terrorismo también podría agregarse a esta lista. No parece una idea descabellada cuando, como ya hemos apuntado, existen tratados sobre parcelas concretas del terrorismo; el ciberterrorismo no dejaría de ser uno más de esos sectores a regular.

Sin embargo, carecemos a nivel internacional de una definición comúnmente aceptada de lo que se entiende por terrorismo -lo que significa que tampoco la hay de ciberterrorismo-. El acuerdo entre los Estados en este punto siempre ha sido imposible y la razón que se apunta de forma reiterada es que "quien es un terrorista a los ojos de unos es un luchador por la libertad a los de otros".

La definición de terrorismo ha supuesto un obstáculo insalvable para la adopción de una convención global sobre este fenómeno. Todos los tratados internacionales al respecto o

DOI: 10.17103/reei.29.07

bien son sectoriales, o bien regionales. En los primeros se obvió deliberadamente el problema de la definición, mientras en los segundos se incluyeron conceptos que sirven exclusivamente a los países de esa determinada región del mundo.

A pesar de ello, el terrorismo es un problema global que necesita del esfuerzo conjunto de toda la comunidad internacional. Del mismo modo que los terroristas colaboran entre sí, debería existir una cooperación entre quienes constituyen sus objetivos reales y potenciales. Pero esta cooperación no puede darse al margen del sistema, esto es, diseñando reducidas coaliciones que funcionen autónomamente sin contemplar si quiera la posibilidad de apelar a las Naciones Unidas. Existiendo una organización cuasi universal como la ONU, no es necesario acudir a alianzas parciales, que recuerdan demasiado a tiempos pretéritos que desembocaron en amargos conflictos. El contraataque directo señalando a Estados patrocinadores que pertenecerían al "eje del mal" o violando la soberanía territorial de otros para realizar operaciones antiterroristas[60] no son soluciones conforme al Derecho Internacional. Esta práctica, muy asentada en la política norteamericana, no debería contagiarse -como está ocurriendo con la ofensiva contra el EI- al resto de los países de la comunidad internacional.

Al igual que en el caso del terrorismo físico, las conductas terroristas que utilizan la tecnología informática también deberían tener un tratamiento internacional. A nuestro entender se hace urgente, por tanto, una respuesta regulatoria a nivel de la comunidad internacional en su conjunto que debería ser promovida desde la organización universal principal: las Naciones Unidas.

3. Otras alternativas para solucionar el problema del ciberterrorismo

Hay quien aboga por que sea la costumbre la fuente de donde vaya emanando la legislación del ciberespacio, sin necesidad de dictados de ninguna autoridad, ya que al no existir una autoridad centralizada única, es más fácil que vayan surgiendo reglas de conducta que se basarían en el consentimiento que los usuarios muestran al utilizar la red[61]. Aunque la costumbre como fuente del Derecho no tiene apenas importancia en el Derecho interno de muchos Estados, es cierto que a nivel internacional sigue siendo una de las dos fuentes autónomas de este ordenamiento[62], a la vez que numerosas convenciones resultan de la codificación de la costumbre internacional.

---

[60] El caso de la captura de un avión egipcio por parte de la Delta Force estadounidense en territorio italiano a raíz del secuestro del Achille Lauro en 1985 podía haber provocado un grave conflicto internacional, al igual que la más reciente operación llevada a cabo por los Navy Seals americanos en mayo de 2011 en Abbottabad, territorio paquistaní, con el fin de abatir al fundador de Al Qaeda, Osama Bin Laden.

[61] Por ejemplo, GOLDSMITH, J. and LESSING, L., *Grounding the Virtual Magistrate*, en http://www.umass.edu/dispute/ncair/groundvm.htm, (última consulta 10 diciembre 2014).

[62] Convenimos con el profesor Pastor Ridruejo en que las dos únicas fuentes del Derecho Internacional realmente autónomas entre las mencionadas por el artículo 38 del Estatuto del Tribunal Internacional de Justicia son la costumbre y los tratados; PASTOR RIDRUEJO, J.A., *Curso de Derecho Internacional Público y Relaciones Internacionales*, Tecnos, Madrid, 2013, p. 65. Véase también FRIEDMAN, W., "General Course in Public International Law", *Collected Courses of The Hague Academy of International Law*, vol. 127, 1969, p. 136.

DOI: 10.17103/reei.29.07

Sin embargo, teniendo una organización internacional que, en este caso, puede asumir el rol de autoridad centralizada a nivel internacional, sería mejor que la ONU o alguno de sus organismos especializados dictaran al menos los principios básicos. Ello no significa que una vez contenidos dichos principios en un tratado internacional, no puedan dar lugar a unas normas consuetudinarias que deban cumplirse por todos los Estados de la comunidad internacional, incluidos los que no sean parte del mencionado tratado. Además, no hay que olvidar que la legislación del ciberespacio no parte de cero. Aquí estamos tratando de reprimir conductas que ya son penalmente reprobables en el mundo físico, esto es, fuera del mundo virtual.

No parece tampoco muy probable una solución al problema que venga contenida en una Resolución del Consejo de Seguridad de la ONU. Nos referimos a un texto similar a la Resolución 1373 (2001) dictada a raíz de los atentados del 11-S, cuya naturaleza legislativa no resulta discutida[63]. Cabría la posibilidad si se diesen unas circunstancias similares a las que se vivieron en ese momento, lo que no es muy probable –afortunadamente- cuando nos referimos al fenómeno ciberterrorista. La conmoción provocada a la comunidad internacional en su conjunto por tres ataques terroristas llevados a cabo en suelo de uno de los miembros permanentes del Consejo de Seguridad, con las consecuencias dramáticas en cuanto a número de víctimas y destrucción de bienes, no tenía precedentes y, por eso, trascurridos tan solo unos días el Consejo de Seguridad adoptó esta Resolución, sin duda, revolucionaria[64].

Por otra parte, aunque no se discuta el contenido normativo de esta Resolución 1373 (2001), no olvidemos que el Consejo de Seguridad carece de competencia para la codificación y el desarrollo progresivo del Derecho Internacional, pues esa función se asigna a la Asamblea General en el artículo 13.1.a) de la Carta de las Naciones Unidas. Luego, si bien es verdad que el Consejo de Seguridad ha desarrollo excepcionalmente un poder legislativo en el ámbito del terrorismo internacional, también es cierto que no podemos tener en cuenta esta vía como posible solución a los problemas que surgen de la elaboración de un tratado internacional, concretamente de la lentitud del proceso y de la falta de voluntad de algunos Estados en obligarse por él.

Efectivamente, el Consejo de Seguridad aprobó un instrumento obligatorio para todos los Estados miembros de la ONU[65] y con efectos inmediatos. La Resolución imponía a "todos los Estados", independientemente de su relación con el fenómeno terrorista, la adopción de una serie de medidas de naturaleza penal, administrativa y procesal, que exigían cambios legislativos en el derecho nacional.

Sin embargo, una nueva Resolución del Consejo de Seguridad con estas características no supone *prima facie* un cauce plausible para la regulación del fenómeno

[63] Véase TALMON, S., "The Security Council as a World Legislature", *American Journal of International Law*, vol 99, 2005, pp. 176-177; SZUREK, S., "La lutte internationale contre le terrorisme sous l'empire du chapitre VII: un laboratoire normative", *Revue Général de Droit International Public*, vol. 11, nº 1, 2005, pp. 15-16.

[64] HINOJOSA MARTÍNEZ, L., *La financiación del terrorismo y las Naciones Unidas*, Tecnos, Madrid, 2008, p. 176.

[65] Artículo 25 de la Carta de las Naciones Unidas.

DOI: 10.17103/reei.29.07

ciberterrorista. Ni siquiera los posteriores ataques terroristas perpetrados en suelo europeo -el 11-M de Madrid y el 7-J de Londres- provocaron la elaboración de Resoluciones equiparables. Tampoco los más recientes sufridos en París y el Copenhague a principios del año 2015 han desencadenado, desde el punto de vista jurídico internacional, un brío legislativo del Consejo de Seguridad de la ONU.

Por otro lado, la creación de un Comité encargado del ciberterrorismo, que promueva el consenso interestatal en la materia, supondría una estrategia paralela para intentar canalizar la cooperación internacional y avanzar en la determinación de los principios jurídicos básicos a respetar en el ciberespacio. Se trataría de un organismo, afín al que existe para el espacio ultraterrestre, que debería acoger técnicos informáticos y expertos en Derecho y que, tomando el pulso a la voluntad de los Estados podría proponer desde meros códigos de conducta para todos los operadores del ciberespacio, hasta el planteamiento de instrumentos jurídicamente vinculantes que recojan el desarrollo progresivo de las normas[66]. Sin duda, aportaría un impulso notable que no debería desdeñarse, pero sea como paso previo para la elaboración de una norma general, sea como organismo para el estudio y desarrollo de la futura evolución legislativa en este campo, se nos antoja un destacado medio complementario que no resulta absolutamente necesario para el desarrollo de esta labor.

Evidentemente, las cuestiones delictivas y de contenido ilegal deben quedar resueltas a su vez en la legislación interna de cada Estado y estar lo más armonizadas posible con las de otros Estados. Existe, por tanto, una necesidad urgente de cooperación internacional con respecto al contenido ilegal y a las conductas delictivas, pero la responsabilidad no solo recae en las autoridades estatales y las agencias internacionales, sino también en la industria y los usuarios.

No cabe duda de que en este sentido, como ha ocurrido ya en otros sectores –navegación aérea, navegación marítima, utilización de materiales peligrosos o financiación-, la regulación a nivel internacional resulta más eficaz al proyectar una mayor legitimidad hacia todos los participantes en el mundo virtual. Una acogida positiva por parte de estos de una norma con vocación de universalidad se augura más factible que las desiguales normas nacionales. A su vez, marca una tendencia bien definida que hoy puede ser rechazada por algunos Estados, pero nadie garantiza a operadores y usuarios que mañana las autoridades gubernamentales la acojan. Cuando ya existe una regulación clara, a la industria sobre todo, pero también a los usuarios, les puede resultar muy arriesgado cambiar sus servidores a países que no pueden garantizar una permanencia perpetua al margen del sistema.

[66] BALSANO, A.M., "An International Legal Instrument for Cyberspace? A Comparative Analysis with Law of Outer Space", en Fuentes-Camacho, Teresa (ed.), *The International Dimensions of Cyberspace Law*, Ashgate – UNESCO, Aldershot, 2000, p. 142.

DOI: 10.17103/reei.29.07

VI. RESPUESTA GLOBAL AL CIBERTERRORISMO DEL ESTADO ISLÁMICO

La regulación internacional del ciberterrorismo deberá tener en cuenta valores ya consolidados en nuestra concepción de los derechos humanos. El derecho a la libertad de opinión y de expresión, que incluye el de no ser molestado por causa de sus opiniones, el de investigar y recibir información y opiniones y el de difundirlas sin limitación de fronteras, por cualquier medio de expresión, se consagra en la Declaración Universal de los Derechos Humanos de 1948 auspiciada por la ONU[67]. Así mismo, ha sido reafirmado en el Pacto de los Derechos Civiles y Políticos de 1966, según el cual este derecho entraña deberes y responsabilidades especiales por lo que puede estar sujeto a restricciones que, fijadas en la ley, deberán ser necesarias para asegurar el respeto de los derechos de terceros o la protección de la seguridad nacional, el orden público o la salud o la moral públicas[68].

La tentación de despreciar estos derechos en aras de proteger la seguridad puede llegar a ser muy grande cuando hablamos de terrorismo. Con demasiada frecuencia el sentimiento humanista comienza a emborronarse ante amenazas graves a la seguridad. Por ello, es importante un marco internacional que sea capaz de buscar un equilibrio sin desvirtuar valores que nos ha costado tanto trabajo conseguir y proteger adecuadamente.

Dentro del entramado institucional de la ONU, la UNESCO promueve el diálogo sobre los aspectos éticos, legales y socioculturales de las nuevas tecnologías de la información y la comunicación. A través de observatorios permanentes, centros de intercambio de información y grupos de discusión, esta organización busca proteger la libertad de expresión, el acceso universal a Internet, la privacidad y el uso adecuado, a la vez que quiere combatir el crimen y la violencia online. El mandato de favorecer la libre circulación de las ideas por medio de la palabra y la imagen, convierten a esta organización en la más adecuada para formular los principios fundamentales del ciberespacio a nivel internacional, buscando un equilibrio, sin duda difícil, entre esos intereses fundamentales que acabamos de exponer[69] y las razones de seguridad[70].

Precisamente ese difícil equilibrio entre libertad y seguridad se plantea de una manera patente cuando se trata de terrorismo. Aunque algunos dirigentes aleguen que los ciudadanos están dispuestos a sacrificar parte de su libertad por fortalecer la seguridad, no consideramos que este sea el único camino a tomar en la lucha contra dicho fenómeno.

---

[67] Artículo 19 de la Declaración Universal de los Derechos Humanos.
[68] Artículo 19 del Pacto de los Derechos Civiles y Políticos.
[69] El informe presentado por un grupo de expertos después de la reunión auspiciada por la UNESCO en 1998, señaló como valores trascendentales, entre otros, el principio ético, la libertad de expresión, el acceso a la información y la cooperación internacional para resolver los conflictos de ley y de jurisdicción; UNESCO, *Report to the Director-General of the UNESCO on the International Experts Meeting on Cyberspace Law*. UNESCO, Monte Carlo, 1998, p. 4.
[70] Laqueur se preguntaba si una sociedad democrática puede vencer al terrorismo sin ceder ninguno de los valores centrales del sistema; LAQUEUR, W., "Reflections on Terrorism", *Foreign Affairs*, nº 64, 1986, p. 88.

DOI: 10.17103/reei.29.07

El control sobre los medios o sobre los proveedores de Internet sería muy difícil de implantar en países con una cultura arraigada de protección de los derechos y libertades fundamentales. Coartar injustificadamente la libertad de expresión y el derecho a la información podría, en último término, convertirse en una victoria para el terrorismo. Probablemente el mayor riesgo inherente a las reacciones contra el terrorismo sea el impulso a imitarlo. En demasiadas ocasiones las medidas antiterroristas acaban con derechos y libertades fundamentales conquistados después de descarnadas luchas sociales.

En nuestra opinión, una reacción exagerada hace perder la legitimidad de la respuesta frente al terrorismo o al ciberterrorismo. Por ello, los cierres y prohibiciones de webs y aplicaciones sin más no parecen ser la respuesta acertada a la propaganda online del EI, como tampoco lo es la restricción del acceso a Internet; máxime cuando estas medidas se toman en algunos países pero no en otros, o por determinados proveedores y no por otros[71].

Ninguna de estas respuestas nos parece acertada ni desde el punto de vista jurídico, ni desde el de la eficacia. Unas normas mínimas, concretadas en un tratado internacional que obligue a las partes a adaptar su legislación interna, acabarían con la impunidad en muchos lugares de las conductas ciberterroristas. Los proveedores de red o de servicio, los operadores de contenido, los motores de búsqueda y, en definitiva, todos los usuarios deberíamos adecuar nuestro comportamiento virtual a dichas normas. Y si ese acuerdo se hace bajo los auspicios de la ONU, teniendo muy presentes los valores que promueve la UNESCO, entre los que destacan la libertad de expresión y el derecho a la información[72], garantizaremos una adecuada protección de los mismos.

En esos principios debería estar incluido que las autoridades nacionales tienen el derecho a declarar que cierto material online es ilegal, por ejemplo, porque está relacionado con actividades terroristas, y pueden adoptar medidas contra proveedores o poseedores de dicho material. Y se admitirá que existen algunas normas morales aceptadas universalmente que tienen que ser reconocidas como parte de cualquier regulación, nacional o internacional, del ciberespacio como, por ejemplo, la de prohibir la producción y la diseminación de información con el propósito de amparar el terrorismo o fomentar el odio racial, étnico o religioso.

[71] Algunas redes sociales constantemente eliminan perfiles y cuentas vinculados a actividades terroristas, aunque las características y la estructura de muchas de ellas incluso facilitan la difusión de contenidos que pueden resultar delictivos. Existen incluso grupos de hacktivistas que pretenden realizar ataques contra las páginas webs de los Estados que supuestamente apoyan al EI. Por ejemplo, Anonymous amenazó con iniciar la operación NO2ISIS, que consistía en una serie de ataques de denegación de servicio contra las webs oficiales de aquellos Estados "patrocinadores" de esta organización terrorista.

[72] Principle no. 1: "The right of communication is a fundamental human right". Principle No. 2: "Every citizen should have the right to meaningful participation in the information society". Principle No. 3: "States should promote universal services where, to the extent possible given the different national and regional circumstances and resources, the new media shall be accessible at community level by all individuals, on a non-discriminatory basis regardless of geographic location"; UNESCO, op cit., p. 6.

DOI: 10.17103/reei.29.07

Los filtros de contenido o la autoregulación a través de códigos de conducta, estatutos de consumidores u orientaciones generales (*guidelines*) que muchos proveedores y usuarios ya desarrollan en sus comunicaciones cibernéticas no son suficientes y, además, no serían en ningún caso incompatibles con unos mecanismos regulatorios mínimos de carácter genérico establecidos para toda la comunidad internacional en su conjunto que, sin duda, ejercerán su influencia en la ética del código.

Actuando en primer lugar en el plano de la regulación, simultáneamente, o quizás en segundo lugar, se podrían considerar las cuestiones que tienen que ver con la aplicación de dicha normativa.

En esta área no hay necesidad de innovar en exceso, ya que como ocurre en muchos de los instrumentos sectoriales contra el terrorismo internacional, apelar a la obligación de los Estados de juzgar o extraditar (*aut dedere aut judicare*) a las personas autoras de estos delitos que se encuentren en su territorio, parece una buena solución también para el ciberterrorismo.

En la última cumbre mediterránea que tuvo lugar en Barcelona y en la que se trató de forma especial el terrorismo yihadista, la representación española sugirió la idea de crear un tribunal internacional para juzgar a los responsables de las actividades terroristas. Traer a colación esta vieja idea –surgió por primera vez en la Sociedad de Naciones, tras el asesinato del rey Alejandro I de Yugoslavia en 1934- como si fuera una propuesta novedosa y original, resulta cuando menos llamativo teniendo en cuenta que en la actualidad disponemos de una Corte Penal Internacional permanente, cuya jurisdicción podría ser ampliada para abarcar expresamente los supuestos de terrorismo internacional, donde quedaría encuadrado también el ciberterrorismo[73]. Se podría aducir la falta de voluntad de los Estados miembros del Estatuto de Roma de 1998 para realizar dicha ampliación. No obstante, este mismo argumento se nos antoja el más probable para oponerse a la creación de un tribunal internacional desde cero que se ocupe exclusivamente de las actividades terroristas[74].

[73] Recordemos que la Corte Penal Internacional ya tiene competencia sobre los actos de terrorismo cuando los mismos constituyan crímenes de guerra, crímenes contra la humanidad o genocidio. Véase INSTITUT CATALÀ INTERNACIONAL PER LA PAU, "El futuro de la Corte Penal Internacional", Documents 09, 2012, p. 59.

[74] Laqueur auguraba que la única forma de que las democracias llevaran a cabo una colaboración global contra el terrorismo es que ocurriera algún desastre de gran envergadura como consecuencia de un acto terrorista. Ese desastre incitaría a "golpear en el centro", es decir, a los principales valedores del terrorismo internacional, a través de una estrategia coordinada a nivel global. Al parecer ni las tragedias del 11-S, el 11-M, el 7-J o los más recientes ataques en Francia, Dinamarca, Nigeria o Kenia, entre muchos otros, se consideran por la comunidad internacional como desastres de gran envergadura que promuevan un consenso en la materia. LAQUEUR, W., *Una historia del terrorismo*, Paidós, Barcelona, 2001, p. 304.

DOI: 10.17103/reei.29.07

VII. CONSIDERACIONES FINALES

Habiendo brotado de la misma fuente que otras organizaciones yihadistas, el EI ha decidido seguir una estrategia mucho más pragmática que ideológica. Gracias a ello ha conseguido hacerse con el control de parte del territorio tanto en Irak como en Siria, a la vez que ha despertado la adhesión de numerosos adeptos en países musulmanes y en occidente.

No se trata de un mero grupo de fanáticos religiosos que se han aprovechado de las circunstancias favorables, sino de un ambicioso proyecto de construcción de un Estado fraguado durante casi una década y que en medio del caos político en Siria e Irak ha sabido hacerse con el liderazgo y proclamar su Califato.

Políticamente pragmático y financieramente perspicaz, el EI fusiona la más extremista ideología islámica con la utilización interesada de las nuevas tecnologías de la información y la comunicación. El EI se vale del potencial de difusión que permite Internet no solo para dar a conocer su proyecto e ideología, sino también para realizar determinadas actividades terroristas.

La propaganda online del EI se enfoca hacia tres objetivos principales: el primero es mostrar, reivindicar, ensalzar y justificar sus acciones; el segundo, reclutar nuevos miembros y forjar alianzas con otras organizaciones; y, por último, amenazar con cometer nuevos actos terroristas en cualquier parte del mundo.

Estas actividades se desarrollan en el ciberespacio, un medio cuya compleja arquitectura impacta directamente en su diseño legal. El gran número de intermediarios que operan en Internet, dando servicios de transmisión, direccionando y recibiendo mensajes es un factor perturbador a la hora de conocer la legislación aplicable y la jurisdicción competente, si es que la hay. Por ello, es necesario un consenso internacional que siente los principios aplicables en la materia.

Si el avance territorial del EI, necesita de una respuesta coordinada internacionalmente, los actos terroristas cometidos en el ciberespacio también deberían tener un freno que supere las fronteras estatales. Pero en ninguno de los casos podemos permitir que la aversión emocional que, de modo natural, inspira el terrorismo suplante una evaluación racional de la situación y una respuesta meditada y acorde a la amenaza que supone el mismo. La línea que distingue contraataque, represalia y venganza no es fácil de establecer cuando el enemigo no puede ser localizado ni identificado con exactitud. Si la respuesta al terrorismo en cualquiera de sus versiones –incluida la digital- no se mantiene dentro de la legalidad internacional, acabará por minar los derechos y libertades fundamentales de las sociedades liberales.

Precisamente en el caso del ciberterrorismo traspasar esa línea puede llevar a conculcar la libertad de expresión y el derecho a la información, por lo que hay que poner especial cuidado a la hora de adoptar medidas en nombre de la seguridad de los ciudadanos.

DOI: 10.17103/reei.29.07

Si en cuanto al avance territorial del EI, consideramos que la ONU debería ser la encargada de desarrollar una potencial ofensiva armada, también para las actividades ciberterroristas, esta organización resultaría la idónea para clarificar la línea infranqueable entre seguridad y protección de los derechos y libertades fundamentales.

La ONU no solo tiene como finalidad primordial preservar la paz y seguridad internacionales, sino que bajo sus auspicios se han adoptado toda una serie de tratados y resoluciones que promueven un alto grado de protección de los derechos humanos. A su vez, dentro de su entramado institucional otros muchos organismos se comprometen con esa protección en sus respectivas áreas temáticas. Así, la UNESCO es la agencia especializada encargada de apoyar los valores generales de la ONU a través de la educación, la ciencia, la comunicación y la información. A nuestro entender, el desarrollo de un cuerpo de principios fundamentales que rijan las actividades en el ciberespacio a nivel internacional debería venir de la mano de la organización universal por antonomasia, teniendo muy presentes los valores que promueve su agencia especializada en torno a la libertad de expresión y el derecho a la información.

No podemos augurar cuál será el futuro del Estado Islámico. Coincidimos con la opinión de la mayoría de los analistas políticos cuando señalan que no tendrá un recorrido muy largo ya que, a pesar de la imagen de poder proyectada en las redes sociales, sus adeptos son un número muy reducido si se tiene en cuenta el territorio que gestiona; no digamos, si atendemos al que pretende someter. No cabe duda de que el apoyo de la población local facilitaría esta labor. Sin embargo, las atrocidades cometidas contra civiles y la intolerancia mostrada hacia otros grupos étnicos y religiosos ha provocado la pérdida de aliados locales.

En cualquier caso, se llamen Al Qaeda en Irak, Estado Islámico o cualquier otro nuevo nombre que elijan, mientras la guerra de Siria siga en curso y las autoridades estatales iraquíes no se hagan fuertes y se consoliden, este tipo de grupos yihadistas radicales continuarán emergiendo. Como apunta Nuñez, no basta con desplegar cazas y eliminar yihadistas por doquier, sin excesiva atención a la legalidad internacional, sino que es primordial impulsar un esfuerzo sostenido en el tiempo y coordinado a nivel internacional. Un esfuerzo que reduzca sustancialmente las crecientes brechas de desigualdad que conducen a la radicalización de muchos individuos que se sienten discriminados y que consideran la violencia como la respuesta a los agravios padecidos, a la vez que se combata en el plano de las ideas esta doctrina extremista, deslegitimando la identificación del Islam con una cultura intrínsecamente indeseable y dando voz y protagonismo a los representantes islámicos[75].

[75] NUÑEZ, J., "Una respuesta inadecuada al desafío del EI", *Política Exterior*, nov-dic., 2014, p. 65.

DOI: 10.17103/reei.29.07